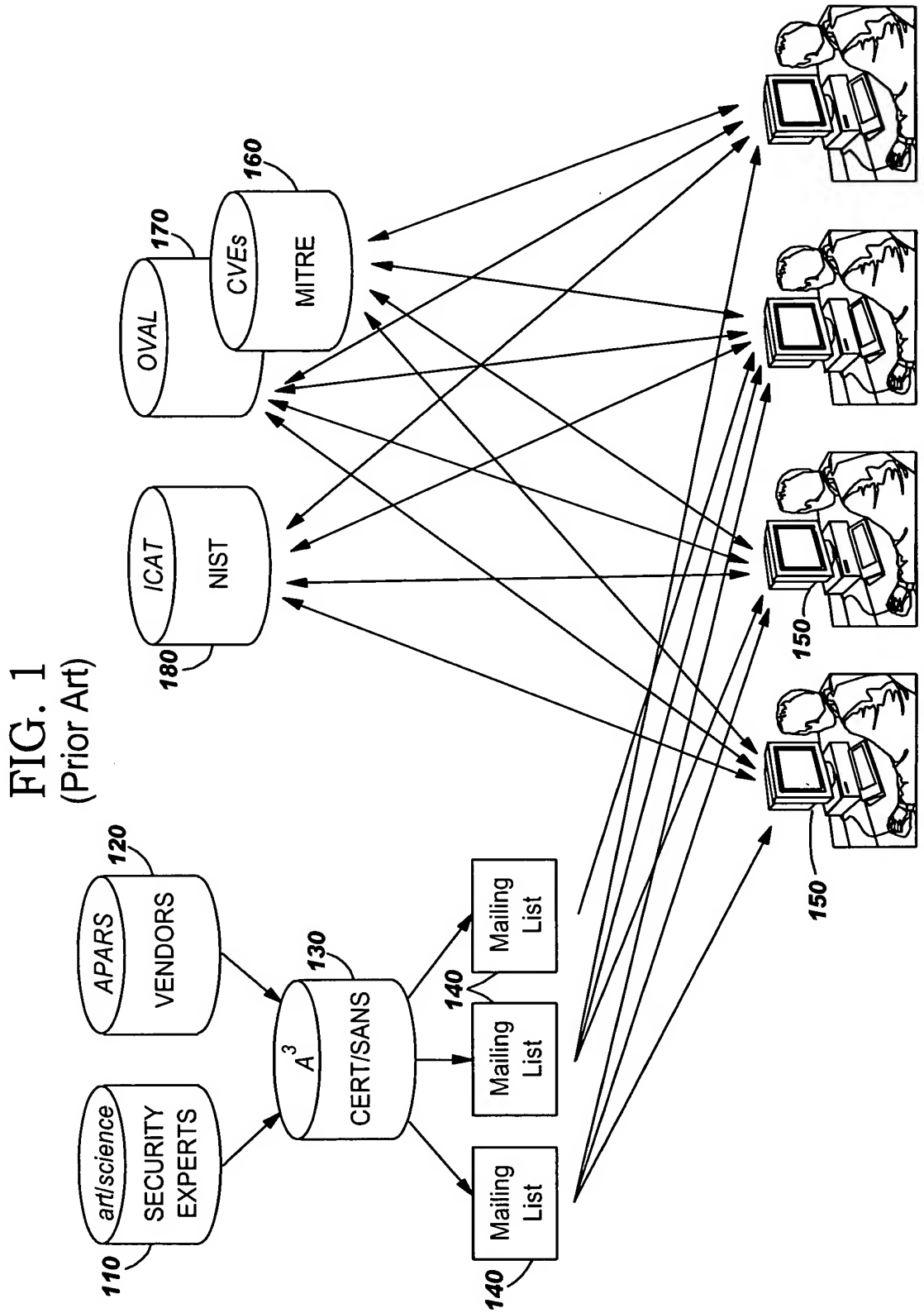


FIG. 1
(Prior Art)

FIG. 2

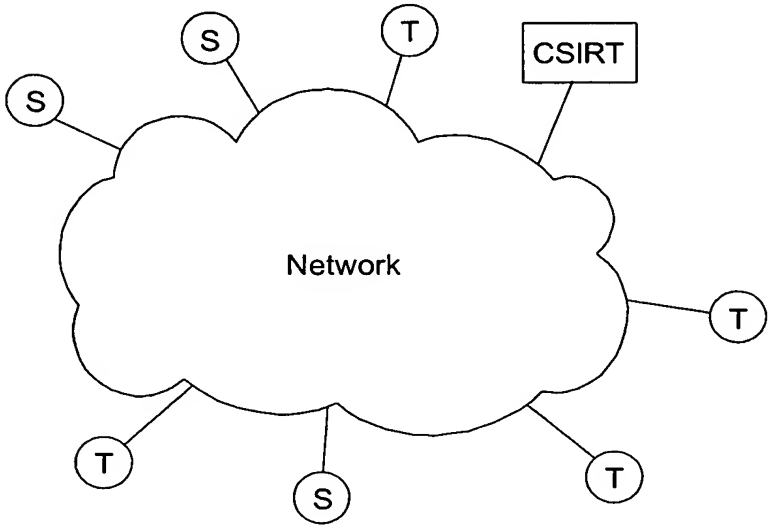


FIG. 3

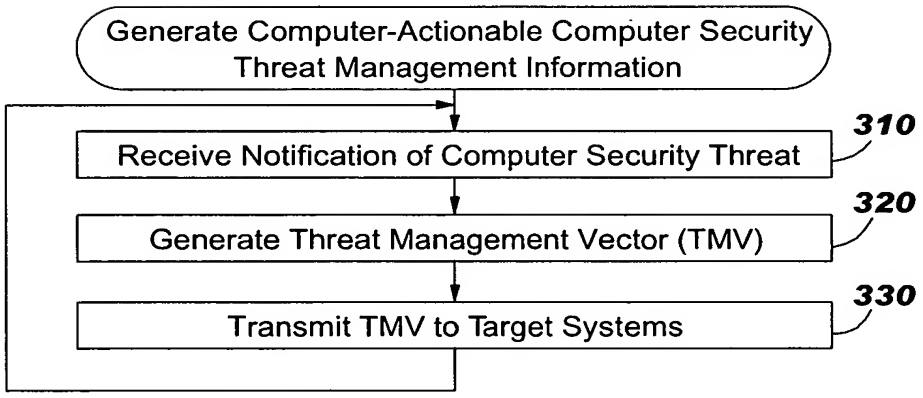


FIG. 4

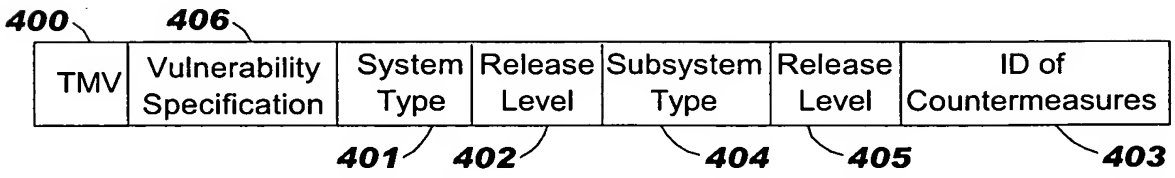


FIG. 5

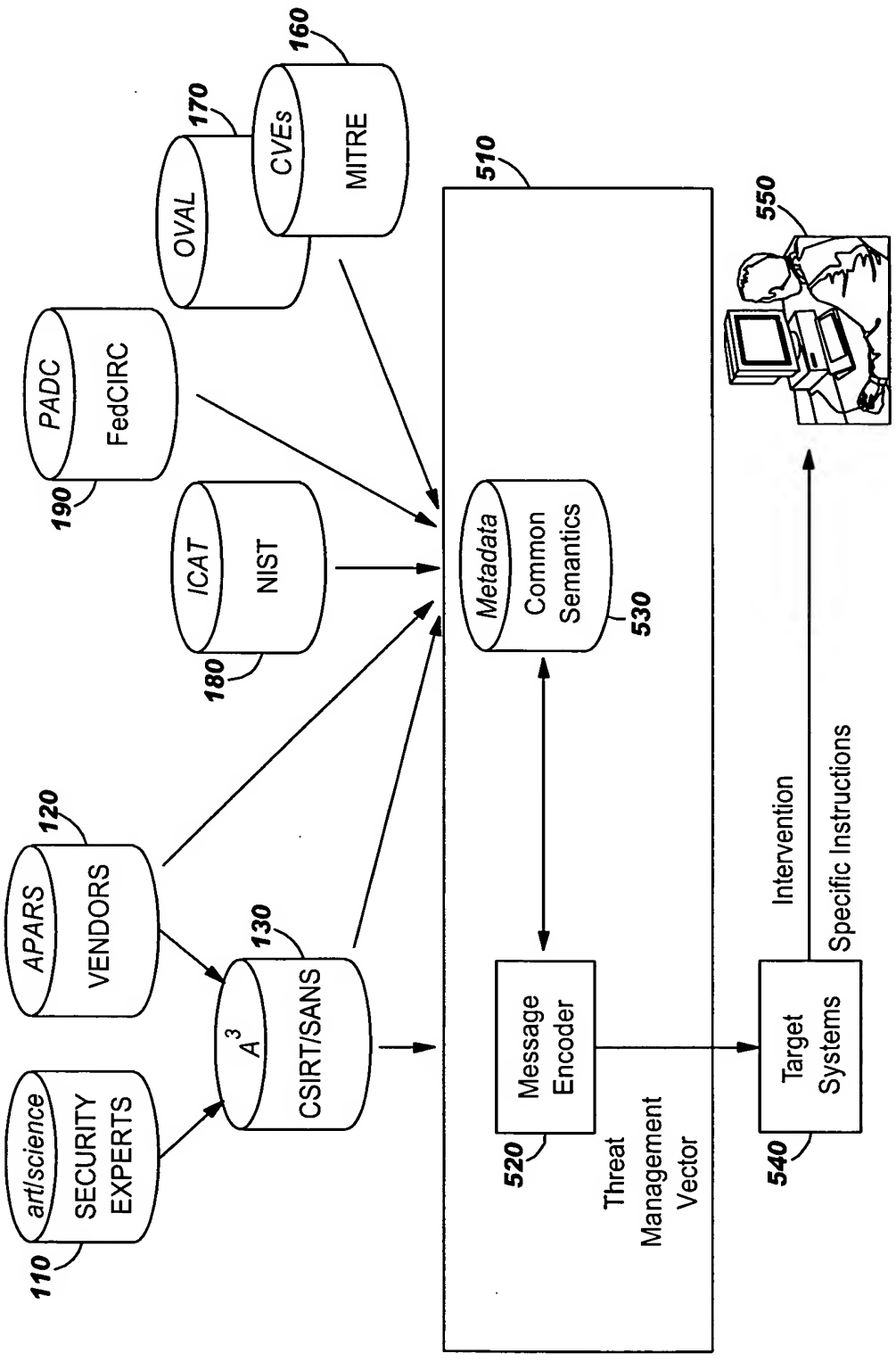

art/science
SECURITY EXPERTS
110
APARS
VENDORS
120
A3
CSIRT/SANS
130
PADC
FedCIRC
190
ICAT
NIST
180
OVAL
CVEs
MITRE
160
170
510
Metadata
Common Semantics
530
Message Encoder
520
Threat Management Vector
Target Systems
540
Intervention
Specific Instructions
550

FIG. 6

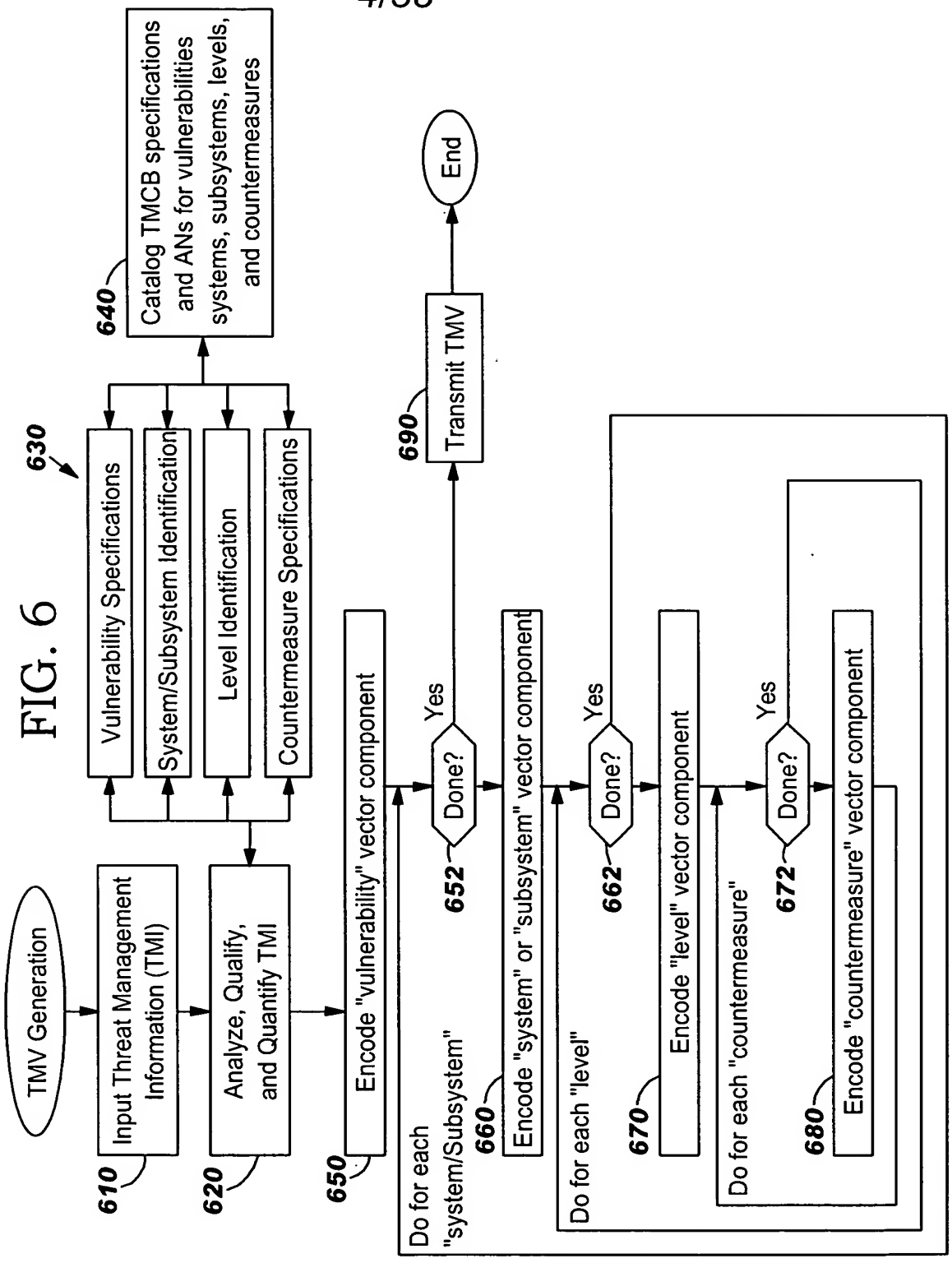

TMV Generation
Input Threat Management Information (TMI)
610
Analyze, Qualify, and Quantify TMI
620
630
Vulnerability Specifications
System/Subsystem Identification
Level Identification
Countermeasure Specifications
640
Catalog TMCB specifications and ANs for vulnerabilities systems, subsystems, levels, and countermeasures
Encode "vulnerability" vector component
650
Done?
652
Yes
Encode "system" or "subsystem" vector component
660
Done?
662
Yes
Encode "level" vector component
670
Done?
672
Yes
Encode "countermeasure" vector component
680
Transmit TMV
690
End
Do for each "system/Subsystem"
Do for each "level"
Do for each "countermeasure"

FIG. 7

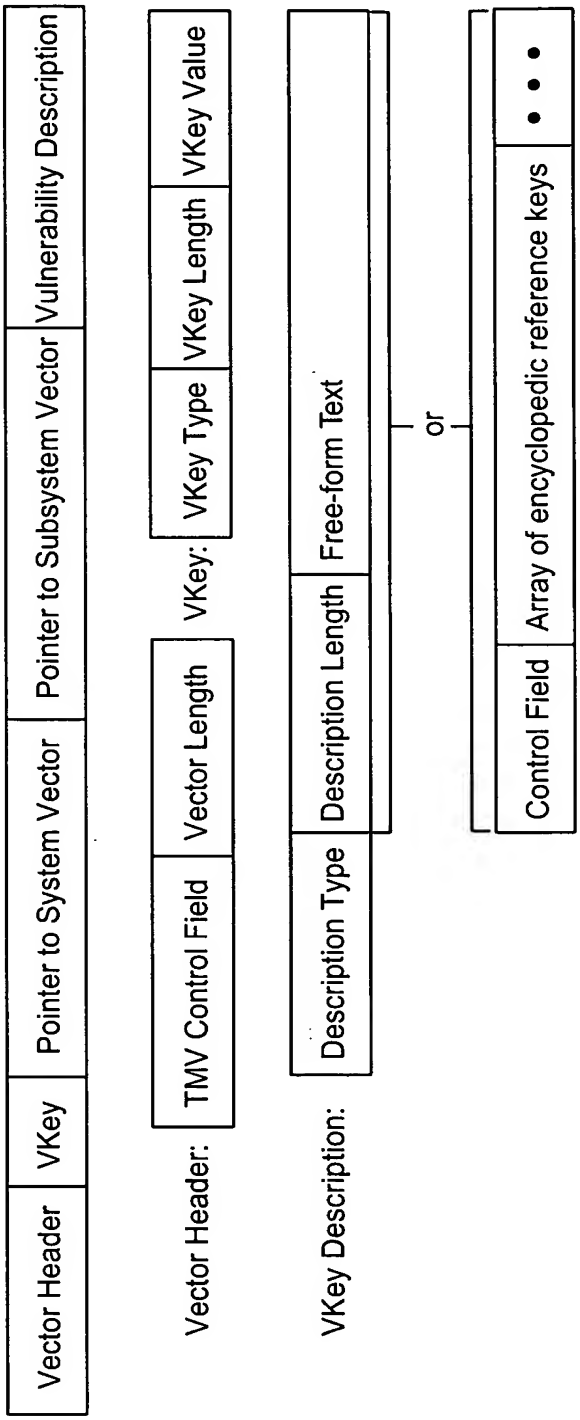

Vector Header
VKey
Pointer to System Vector
Pointer to Subsystem Vector
Vulnerability Description
Vector Header:
TMV Control Field
Vector Length
VKey:
VKey Type
VKey Length
VKey Value
VKey Description:
Description Type
Description Length
Free-form Text
or
Control Field
Array of encyclopedic reference keys
• • •

FIG. 8

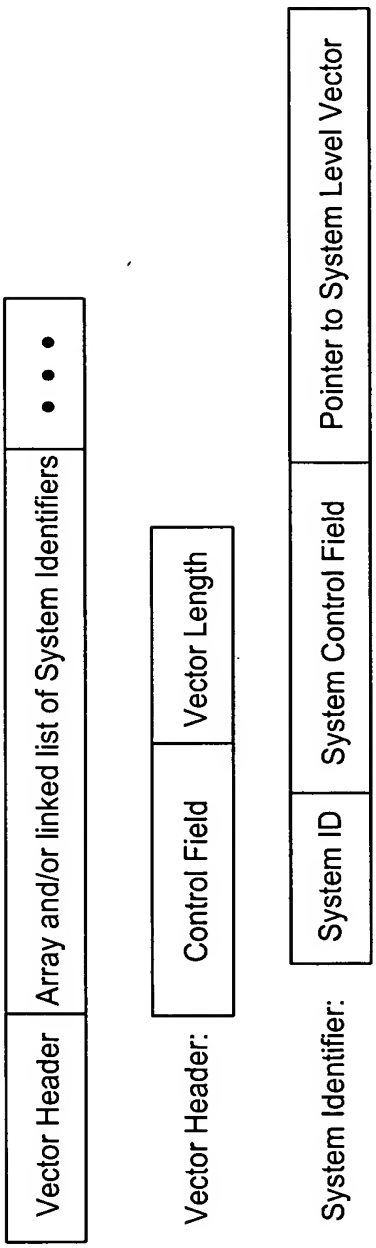

Vector Header
Array and/or linked list of System Identifiers
• • •
Vector Header:
Control Field
Vector Length
System Identifier:
System ID
System Control Field
Pointer to System Level Vector

FIG. 9

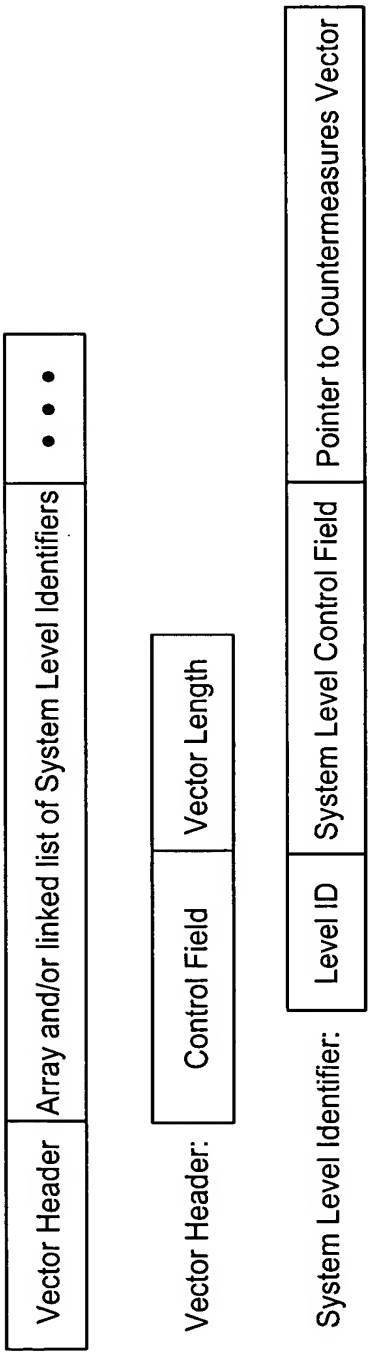
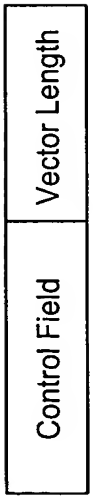

Vector Header
Array and/or linked list of System Level Identifiers
• • •
Vector Header:
Control Field
Vector Length
System Level Identifier:
Level ID
System Level Control Field
Pointer to Countermeasures Vector

FIG. 10

Vector Header:



Countermeasure Metadata:

FIG. 11

Countermeasure Metadata:

FIG. 12

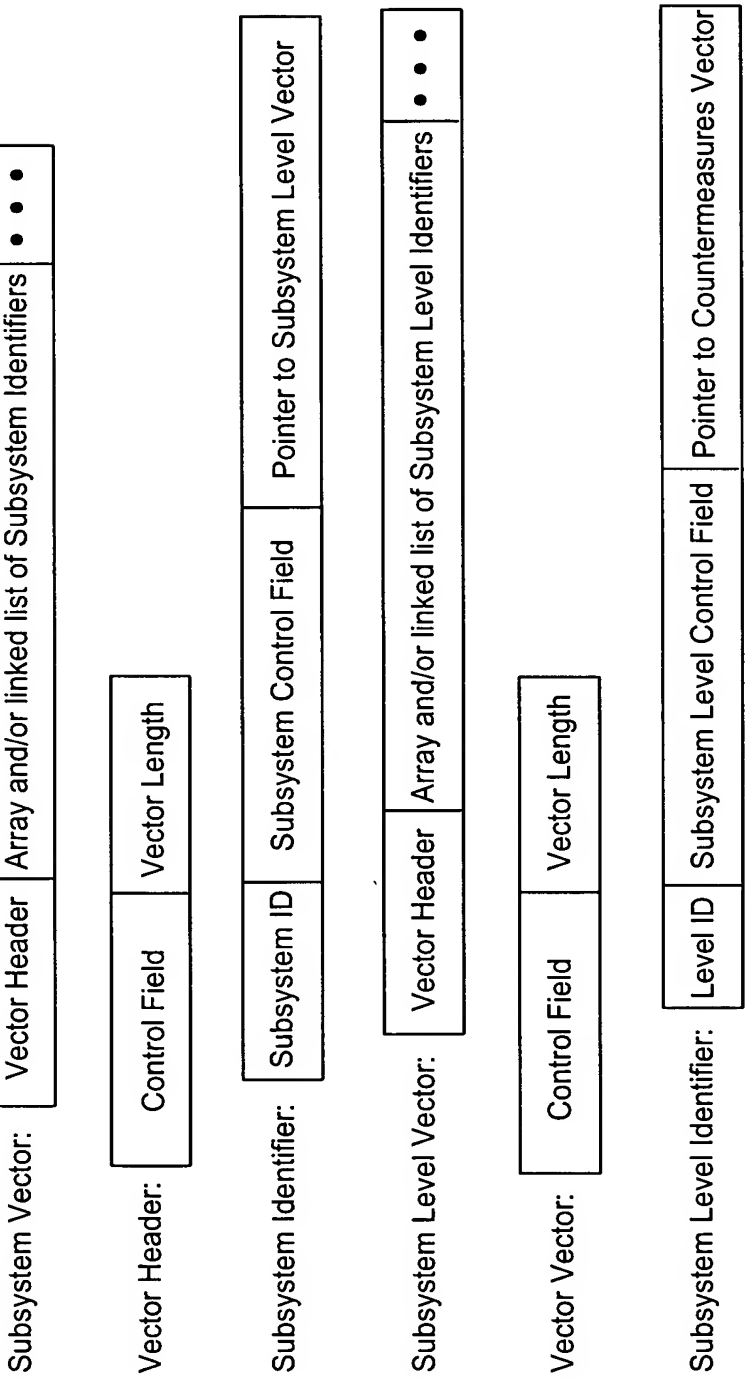

Subsystem Vector:
Vector Header
Array and/or linked list of Subsystem Identifiers
• • •
Vector Header:
Control Field
Vector Length
Subsystem Identifier:
Subsystem ID
Subsystem Control Field
Pointer to Subsystem Level Vector
Subsystem Level Vector:
Vector Header
Array and/or linked list of Subsystem Level Identifiers
• • •
Vector Vector:
Control Field
Vector Length
Subsystem Level Identifier:
Level ID
Subsystem Level Control Field
Pointer to Countermeasures Vector

FIG. 13

System Table (indexed by System ID and System Name):

SystemID (assigned by TMANA)	System Name (from NIST ICAT)	System Level Table

Where System Level Table is defined as:

Level ID (assigned by TMANA)	Version and Release Number (assigned by NIST ICAT or vendors)

Subsystem Table (indexed by Subsystem ID and Subsystem Name):

SubsystemID (assigned by TMANA)	Subsystem Name (from NIST ICAT)	Subsystem Level Table (as above)

Threat Severity Table (indexed by Severity ID and Severity Name):

Severity ID (assigned by TMANA)	Severity Name (from NIST ICAT)

Countermeasure (CM) Table (indexed by CM ID, CM Type, and CM Name):

CM ID (assigned by TMANA)	CM Type (assigned by TMANA)	CM Name (assigned by TMANA)

FIG. 14

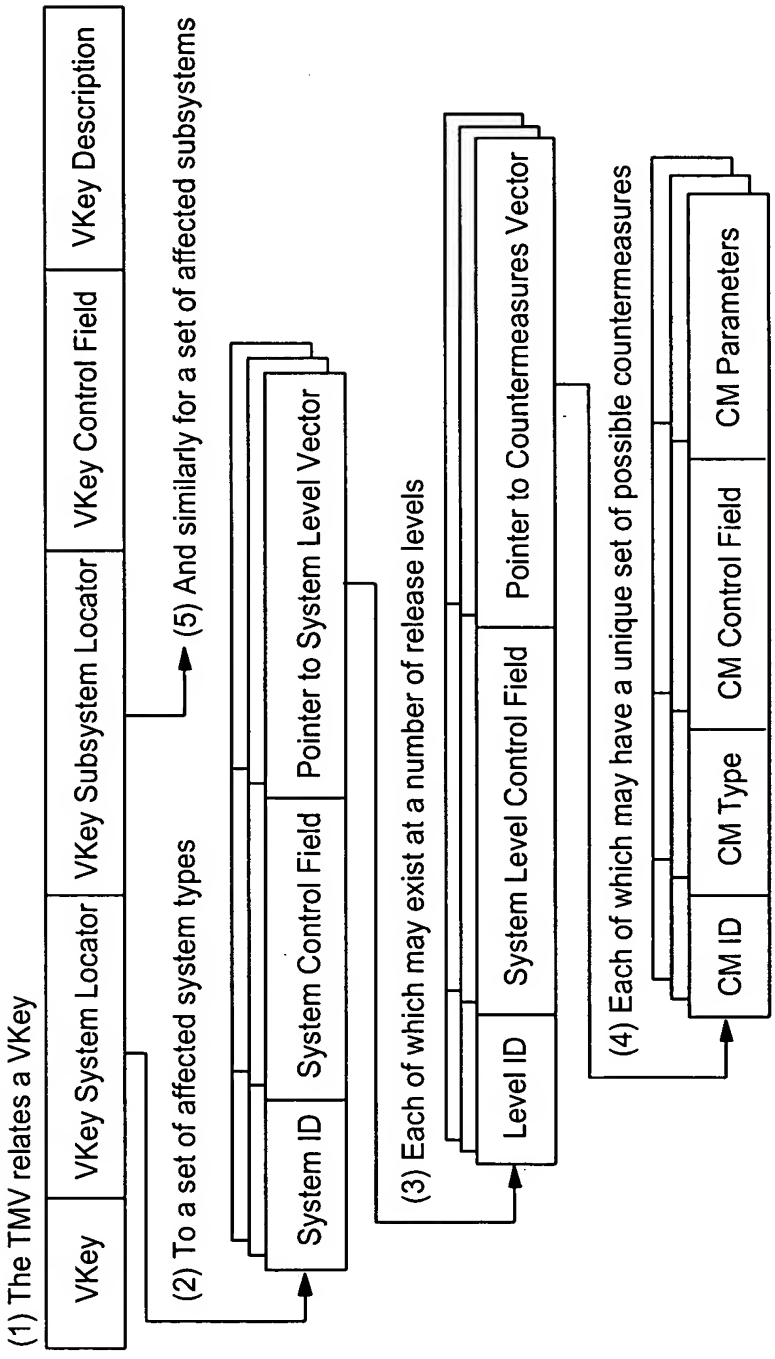

(1) The TMV relates a VKey
VKey
VKey System Locator
VKey Subsystem Locator
VKey Control Field
VKey Description
(2) To a set of affected system types
(5) And similarly for a set of affected subsystems
System ID
System Control Field
Pointer to System Level Vector
(3) Each of which may exist at a number of release levels
Level ID
System Level Control Field
Pointer to Countermeasures Vector
(4) Each of which may have a unique set of possible countermeasures
CM ID
CM Type
CM Control Field
CM Parameters

FIG. 15

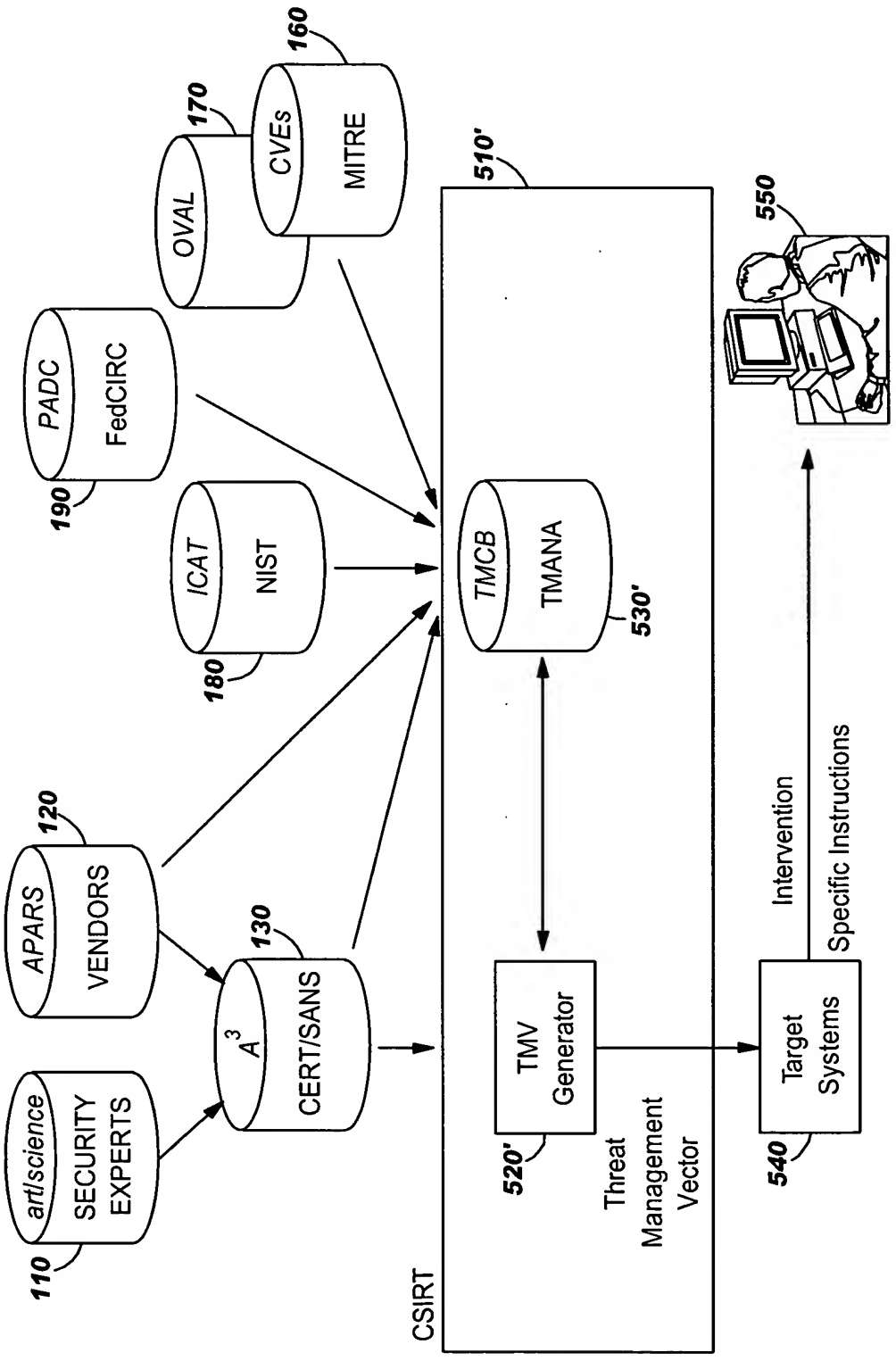

art/science
SECURITY EXPERTS
110
APARS
VENDORS
120
A3
CERT/SANS
130
PADC
FedCIRC
190
ICAT
NIST
180
OVAL
CVEs
MITRE
160
170
CSIRT
510'
TMCB
TMANA
530'
TMV Generator
520'
Threat Management Vector
Target Systems
540
Intervention
Specific Instructions
550

FIG. 16

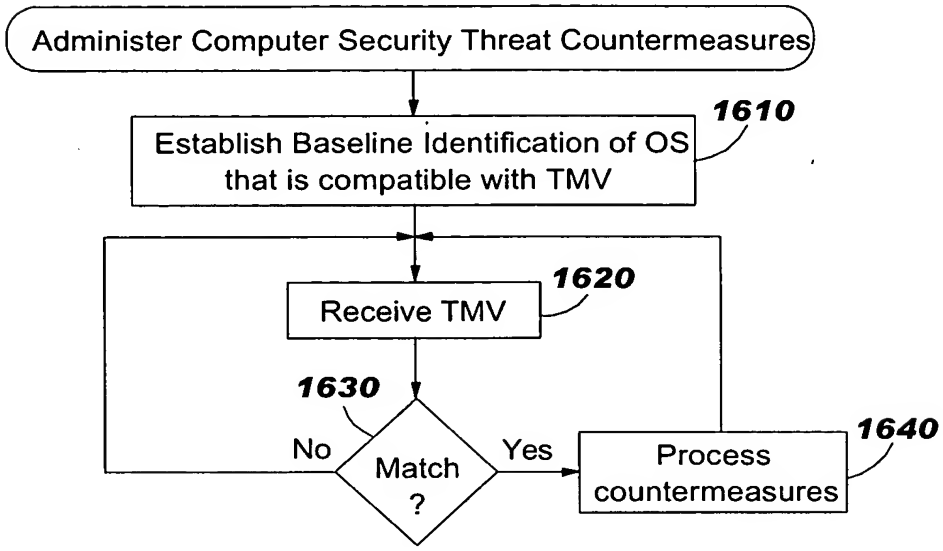

Administer Computer Security Threat Countermeasures
Establish Baseline Identification of OS that is compatible with TMV
1610
Receive TMV
1620
1630
No
Match ?
Yes
Process countermeasures
1640

FIG. 17

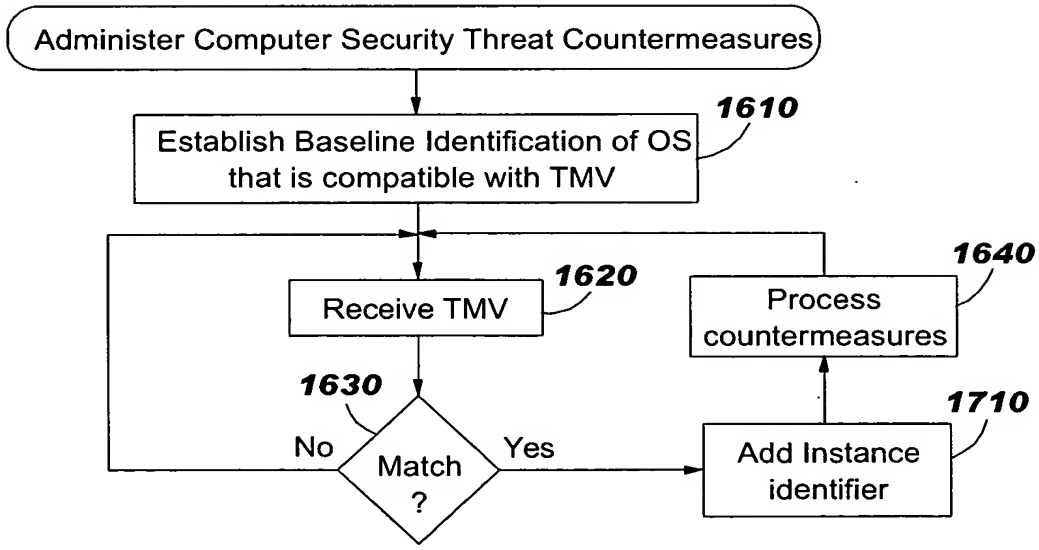

Administer Computer Security Threat Countermeasures
Establish Baseline Identification of OS that is compatible with TMV
1610
Receive TMV
1620
1630
No
Match ?
Yes
Process countermeasures
1640
Add Instance identifier
1710

FIG. 18

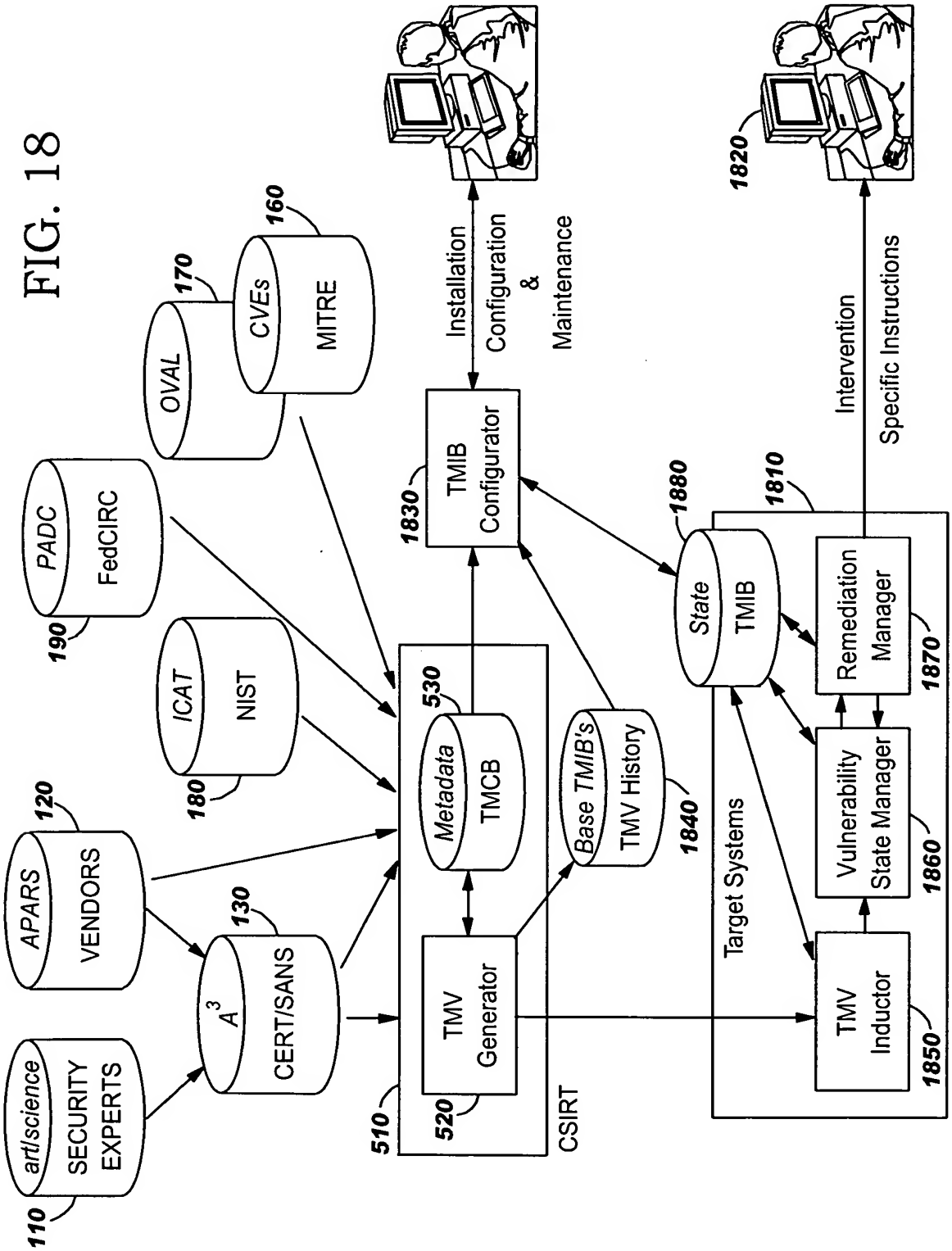

art/science
SECURITY EXPERTS
110
APARS
VENDORS
120
A3
CERT/SANS
130
PADC
FedCIRC
190
ICAT
NIST
180
OVAL
CVEs
MITRE
160
170
Installation
Configuration
&
Maintenance
1830
TMIB Configurator
Metadata
TMCB
530
Base TMIB's
TMV History
1840
TMV Generator
520
510
CSIRT
1880
State
TMIB
1810
Target Systems
Remediation Manager
1870
Vulnerability State Manager
1860
TMV Inductor
1850
Intervention
Specific Instructions
1820

FIG. 19

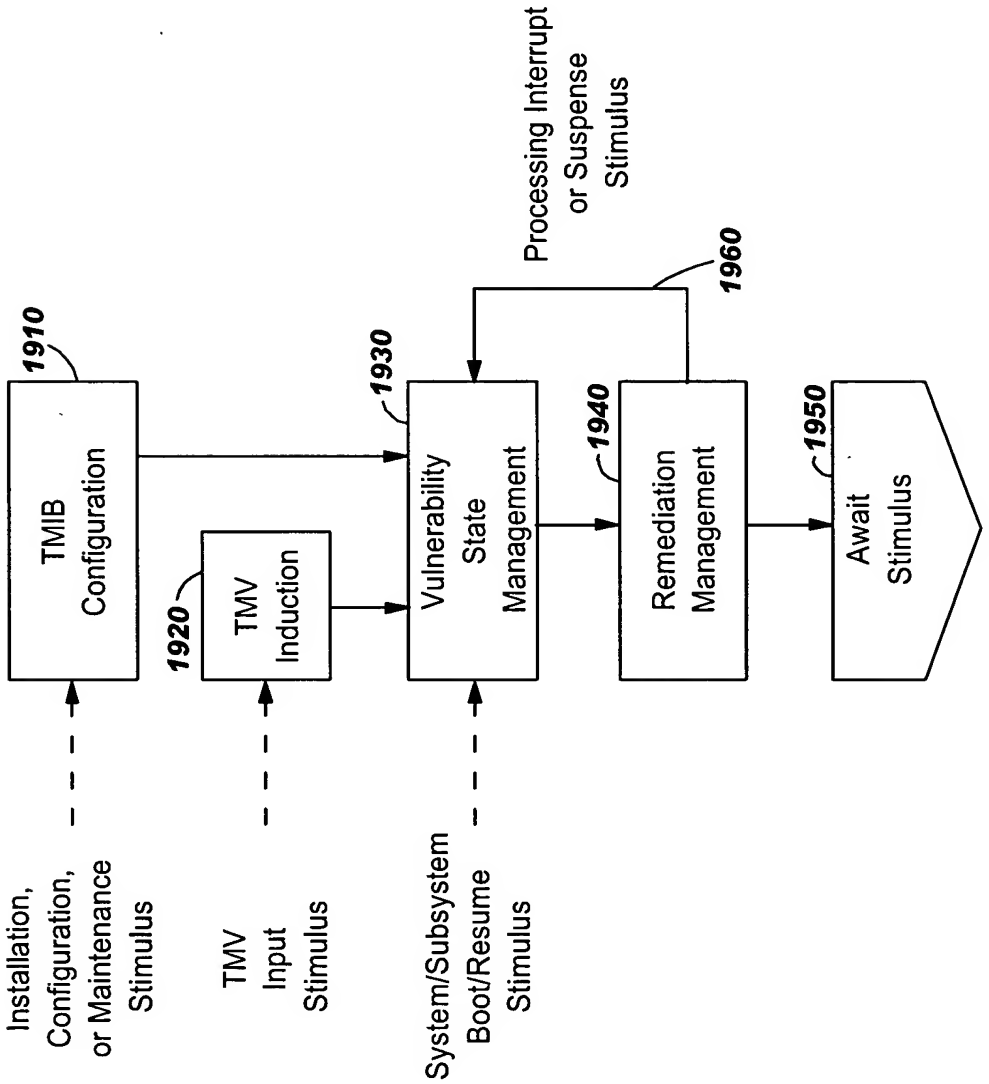

1910
TMIB Configuration
1920
TMV Induction
1930
Vulnerability State Management
1940
Remediation Management
1950
Await Stimulus
1960
Processing Interrupt or Suspense Stimulus
Installation, Configuration, or Maintenance Stimulus
TMV Input Stimulus
System/Subsystem Boot/Resume Stimulus

FIG. 20

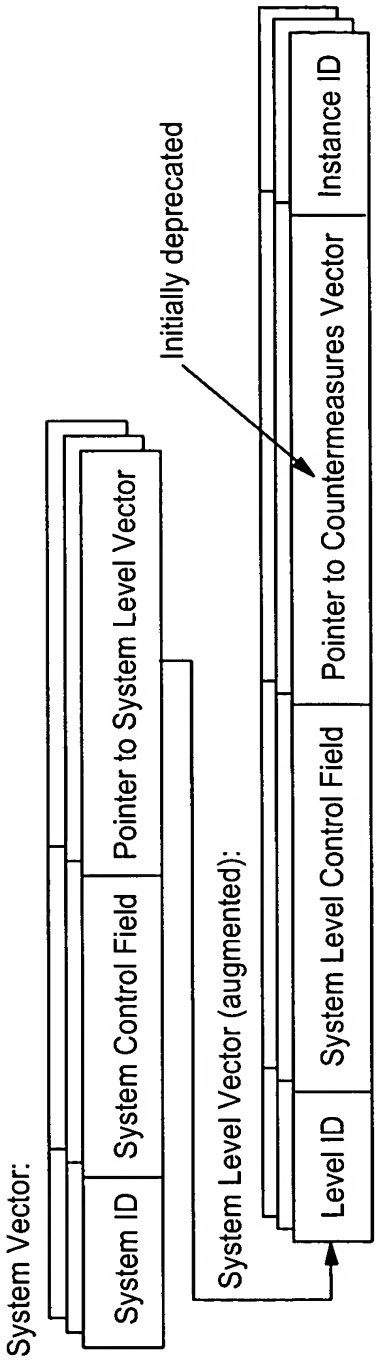

System Vector:
System ID
System Control Field
Pointer to System Level Vector
Initially deprecated
System Level Vector (augmented):
Level ID
System Level Control Field
Pointer to Countermeasures Vector
Instance ID

FIG. 21

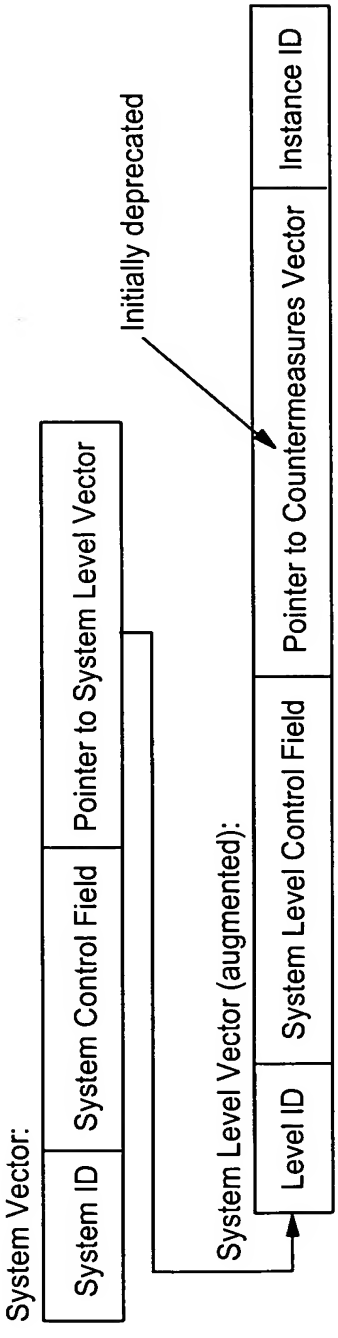

System Vector:
System ID
System Control Field
Pointer to System Level Vector
Initially deprecated
System Level Vector (augmented):
Level ID
System Level Control Field
Pointer to Countermeasures Vector
Instance ID

FIG. 22

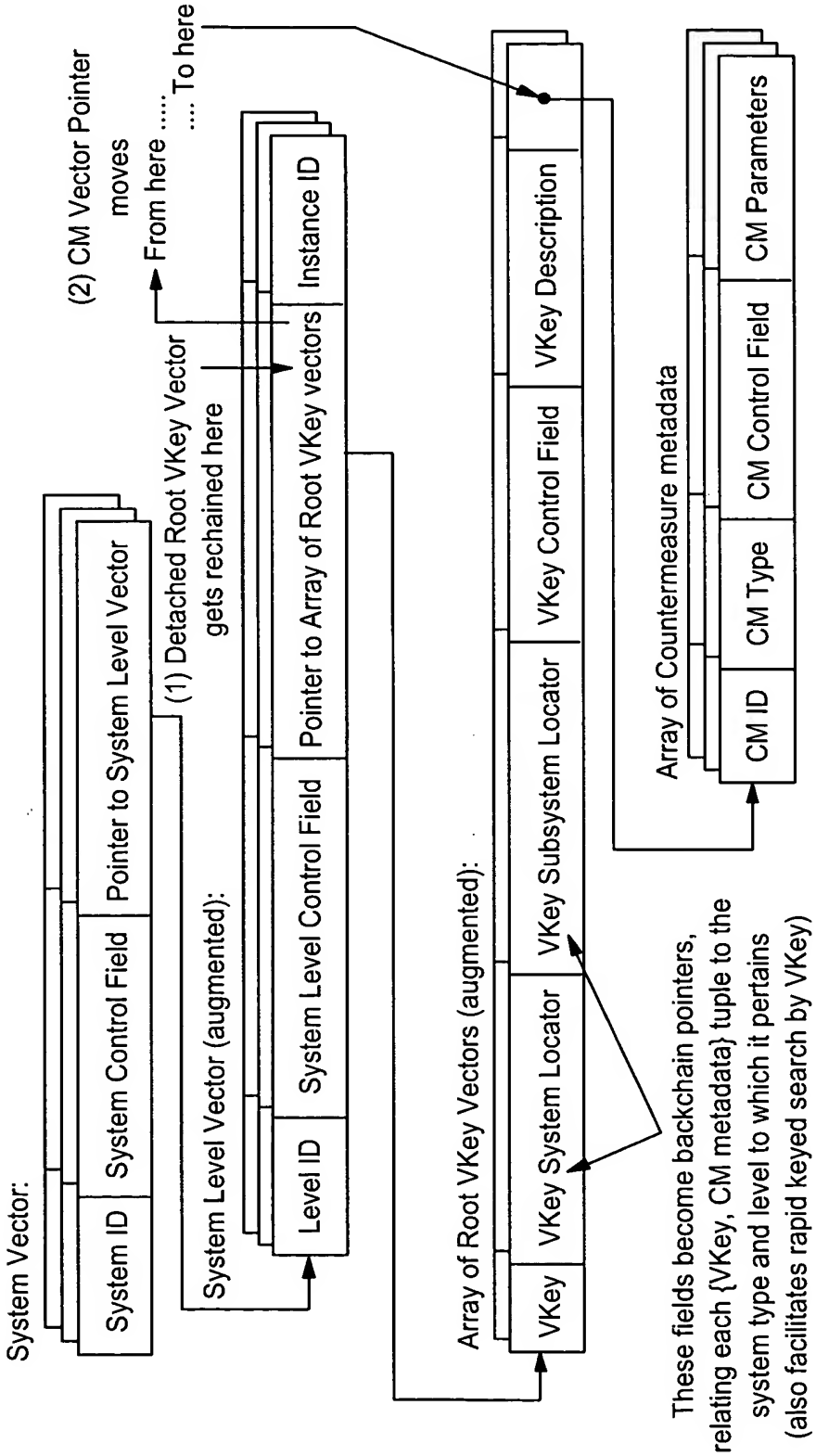

System Vector:
System ID
System Control Field
Pointer to System Level Vector
(1) Detached Root VKey Vector gets rechained here
System Level Vector (augmented):
Level ID
System Level Control Field
Pointer to Array of Root VKey vectors
Instance ID
(2) CM Vector Pointer moves From here .... To here
Array of Root VKey Vectors (augmented):
VKey
VKey System Locator
VKey Subsystem Locator
VKey Control Field
VKey Description
Array of Countermeasure metadata
CM ID
CM Type
CM Control Field
CM Parameters
These fields become backchain pointers, relating each {VKey, CM metadata} tuple to the system type and level to which it pertains (also facilitates rapid keyed search by VKey)

FIG. 23

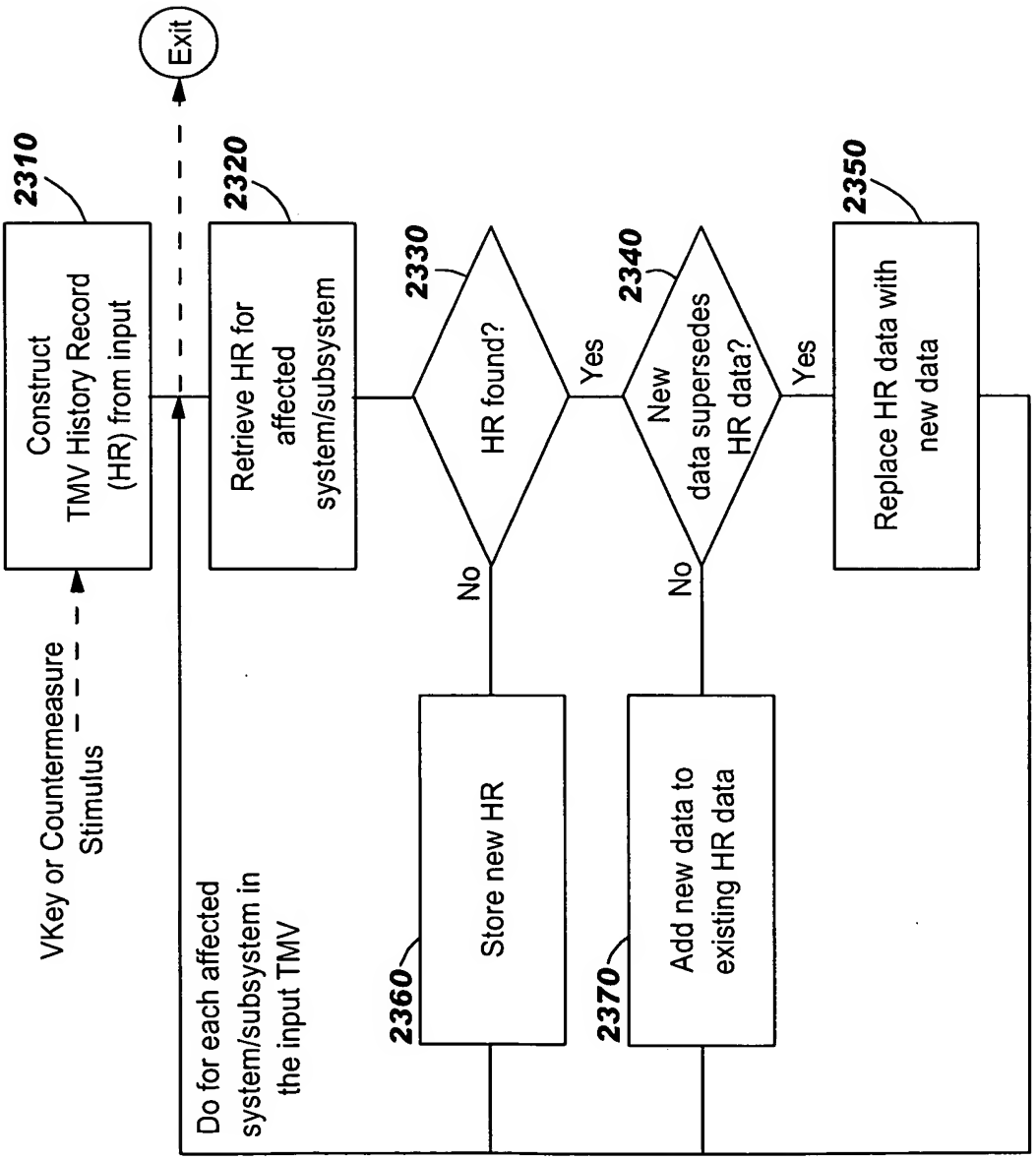

Exit
2310
Construct TMV History Record (HR) from input
2320
Retrieve HR for affected system/subsystem
2330
HR found?
Yes
2340
New data supersedes HR data?
Yes
2350
Replace HR data with new data
No
No
2360
Store new HR
2370
Add new data to existing HR data
VKey or Countermeasure Stimulus
Do for each affected system/subsystem in the input TMV

FIG. 24

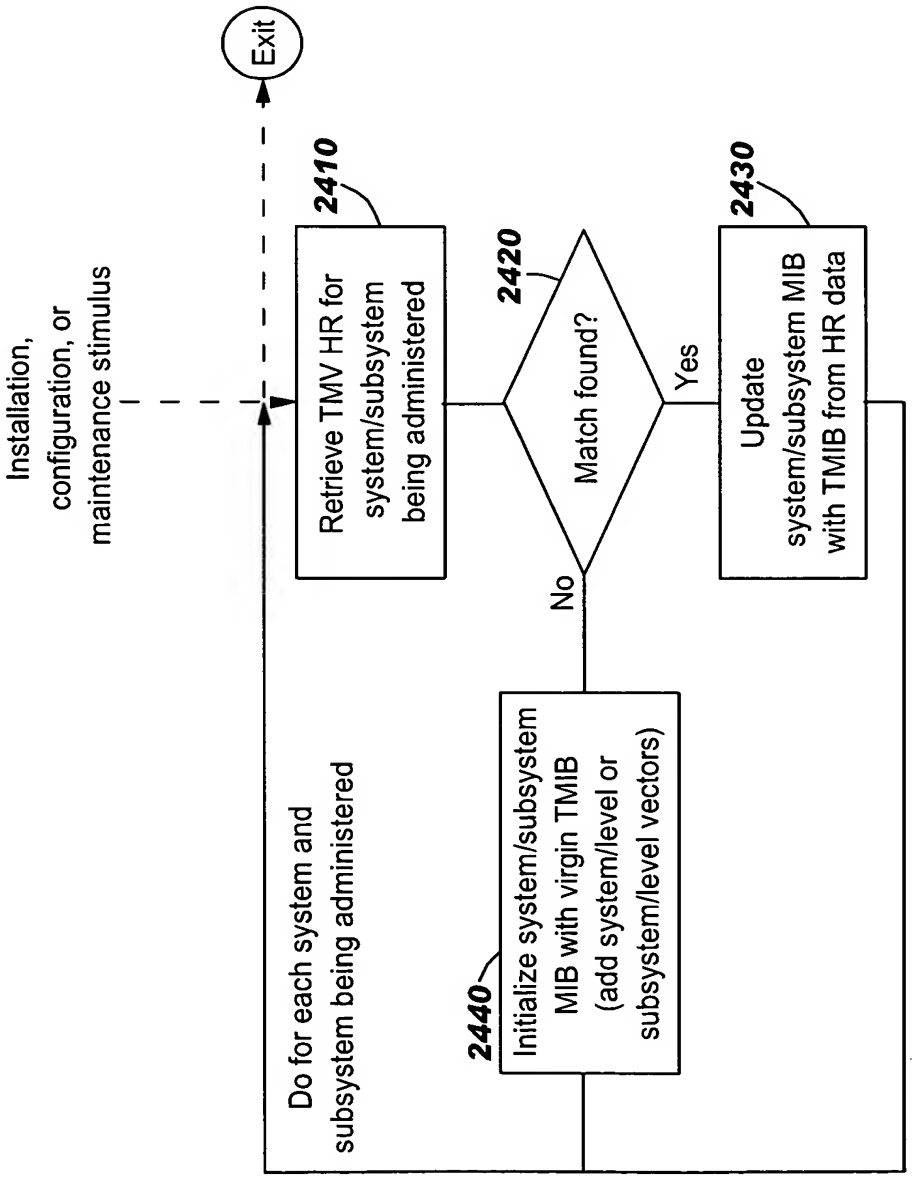

Installation, configuration, or maintenance stimulus
Exit
2410
Retrieve TMV HR for system/subsystem being administered
2420
Match found?
Yes
No
2430
Update system/subsystem MIB with TMIB from HR data
2440
Initialize system/subsystem MIB with virgin TMIB (add system/level or subsystem/level vectors)
Do for each system and subsystem being administered

FIG. 25

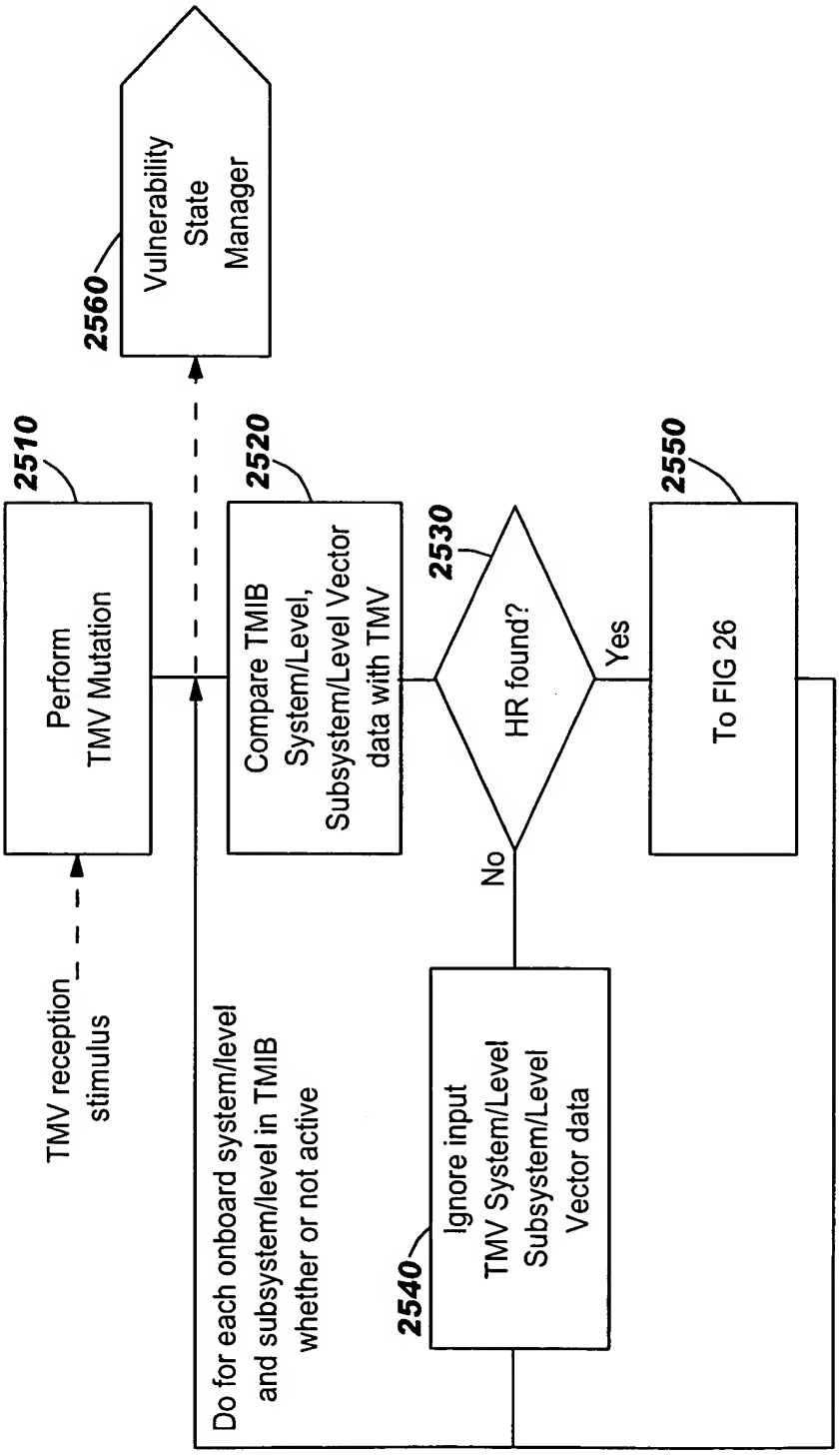

2560
Vulnerability State Manager
2510
Perform TMV Mutation
2520
Compare TMIB System/Level, Subsystem/Level Vector data with TMV
2530
HR found?
Yes
2550
To FIG 26
No
2540
Ignore input TMV System/Level Subsystem/Level Vector data
TMV reception stimulus
Do for each onboard system/level and subsystem/level in TMIB whether or not active

FIG. 26

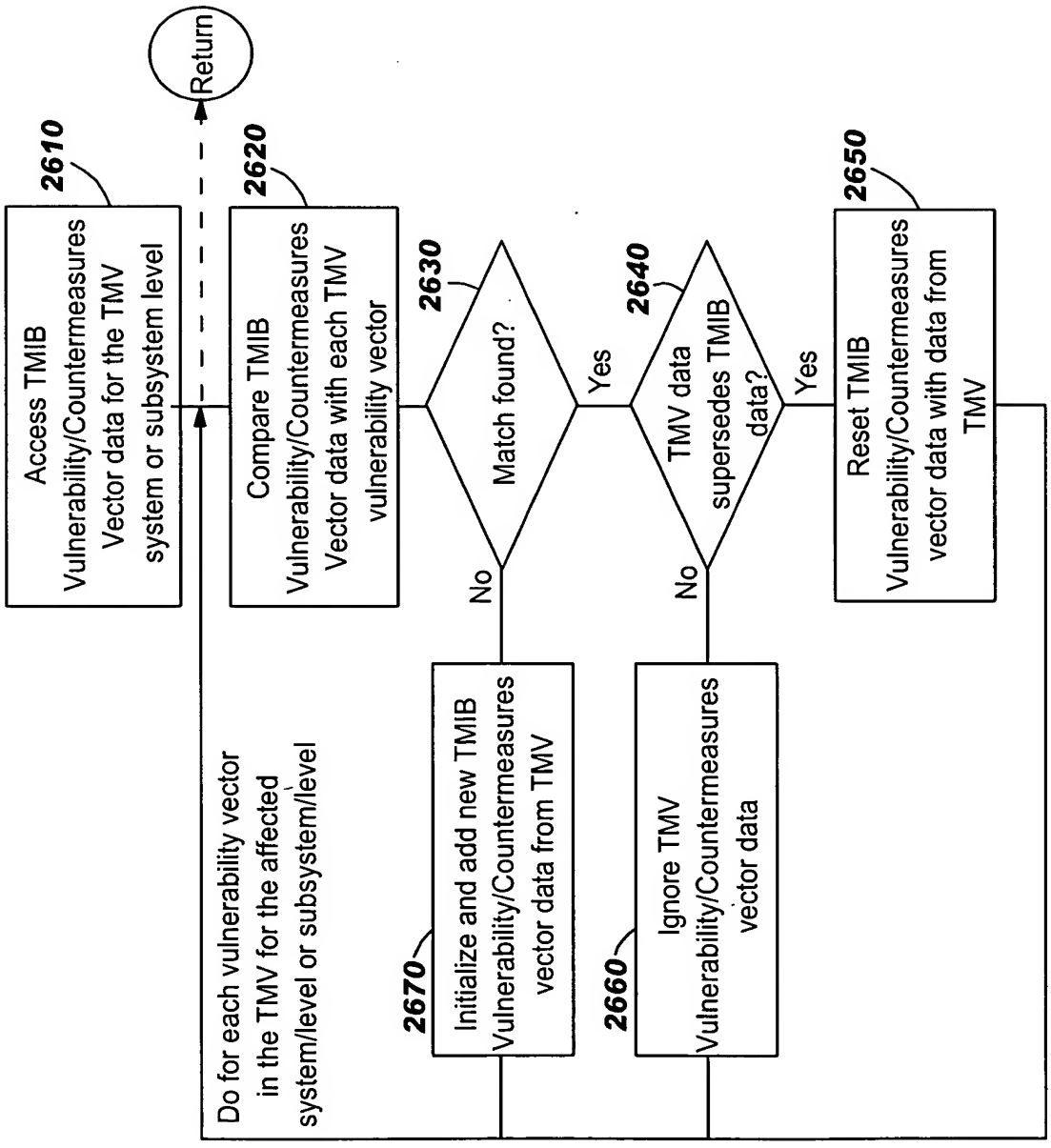

Return
2610
Access TMIB Vulnerability/Countermeasures Vector data for the TMV system or subsystem level
2620
Compare TMIB Vulnerability/Countermeasures Vector data with each TMV vulnerability vector
2630
Match found?
Yes
No
2640
TMV data supersedes TMIB data?
Yes
No
2650
Reset TMIB Vulnerability/Countermeasures vector data with data from TMV
2670
Initialize and add new TMIB Vulnerability/Countermeasures vector data from TMV
2660
Ignore TMV Vulnerability/Countermeasures vector data
Do for each vulnerability vector in the TMV for the affected system/level or subsystem/level

FIG. 27

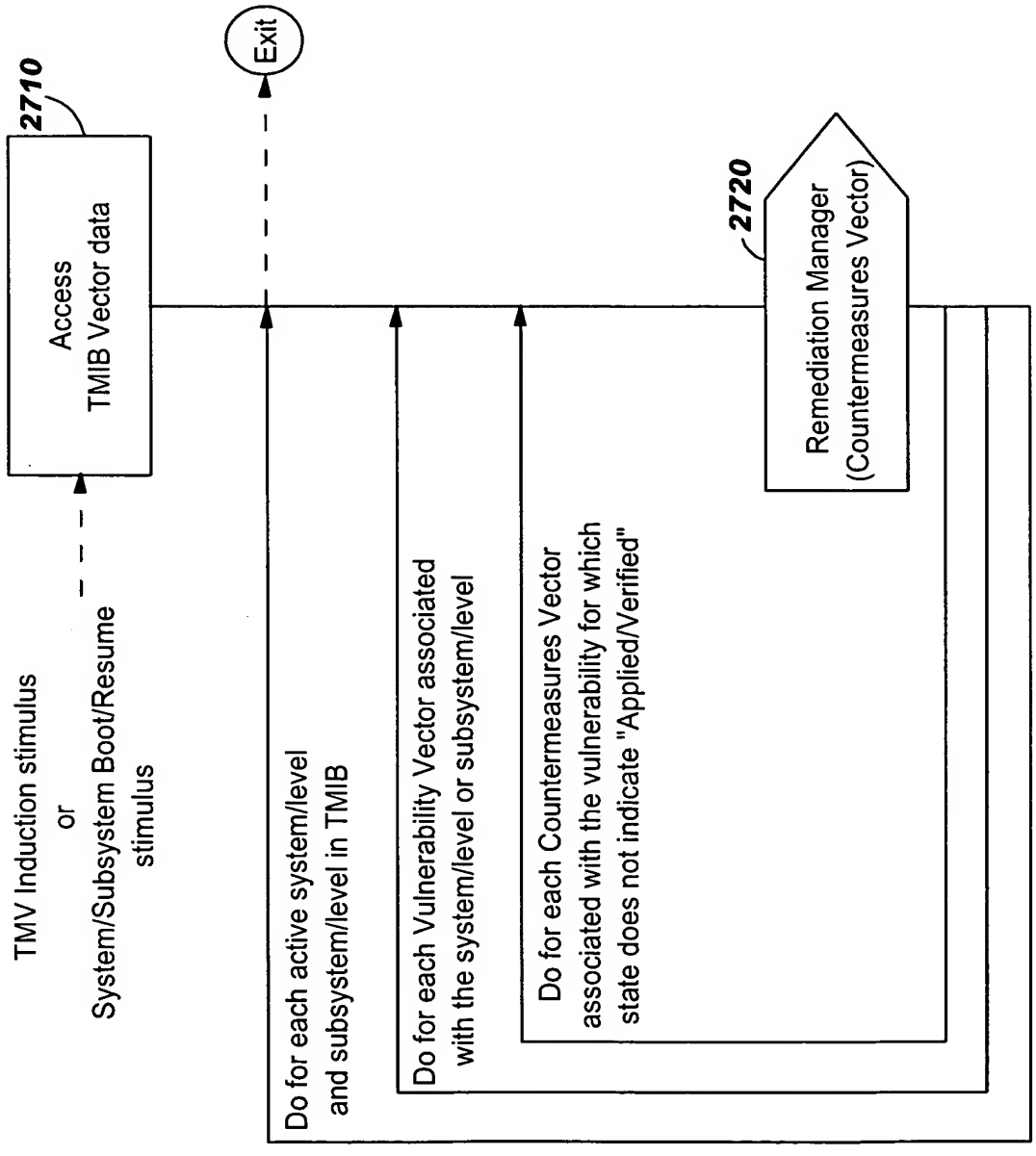

TMV Induction stimulus
or
System/Subsystem Boot/Resume
stimulus
2710
Access
TMIB Vector data
Exit
2720
Remediation Manager
(Countermeasures Vector)
Do for each active system/level
and subsystem/level in TMIB
Do for each Vulnerability Vector associated
with the system/level or subsystem/level
Do for each Countermeasures Vector
associated with the vulnerability for which
state does not indicate "Applied/Verified"

FIG. 28

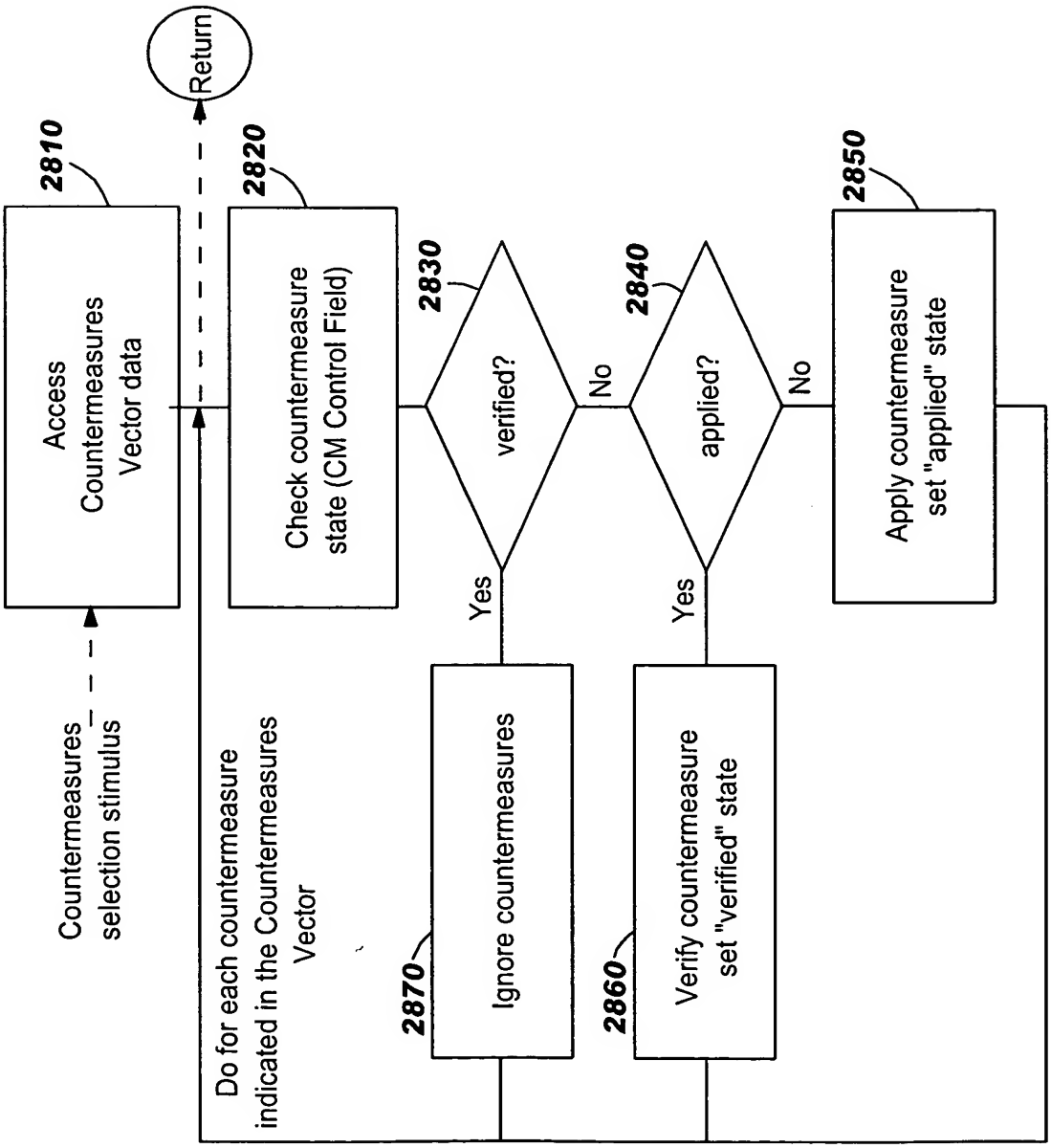

Countermeasures selection stimulus
Access Countermeasures Vector data
2810
Return
Check countermeasure state (CM Control Field)
2820
verified?
2830
No
applied?
2840
No
Apply countermeasure set "applied" state
2850
Yes
Yes
Ignore countermeasures
2870
Verify countermeasure set "verified" state
2860
Do for each countermeasure indicated in the Countermeasures Vector

FIG. 29

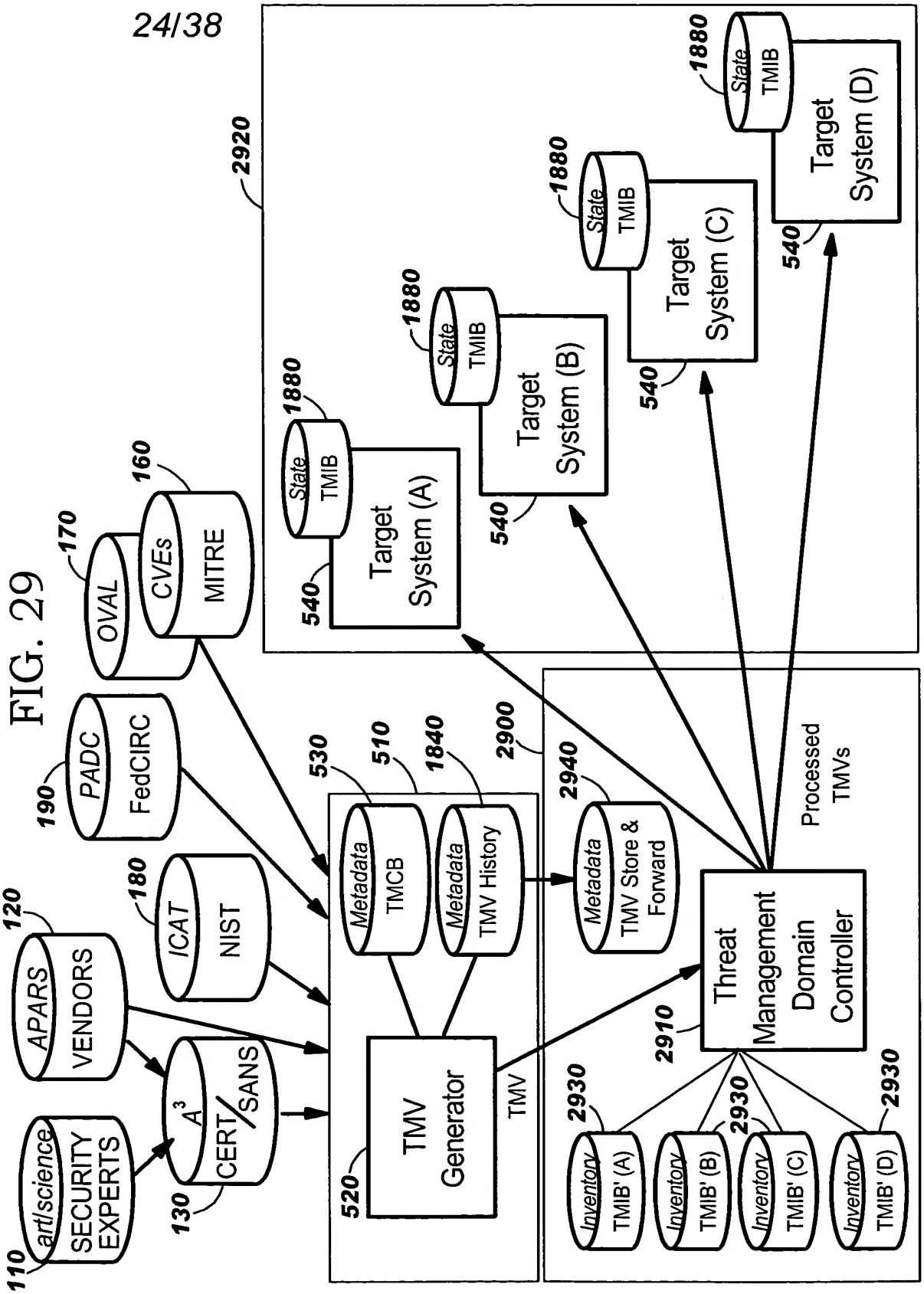

110
art/science
SECURITY EXPERTS
130
A3
CERT/SANS
120
APARS
VENDORS
180
ICAT
NIST
190
PADC
FedCIRC
170
OVAL
160
CVEs
MITRE
520
TMV Generator
530
Metadata
TMCB
510
1840
Metadata
TMV History
2900
2940
Metadata
TMV Store & Forward
TMV
2910
Threat Management Domain Controller
Processed TMVs
2930
Inventory
TMIB' (A)
Inventory
TMIB' (B)
Inventory
TMIB' (C)
Inventory
TMIB' (D)
2920
1880
State
TMIB
Target System (A)
540
Target System (B)
Target System (C)
Target System (D)

FIG. 30

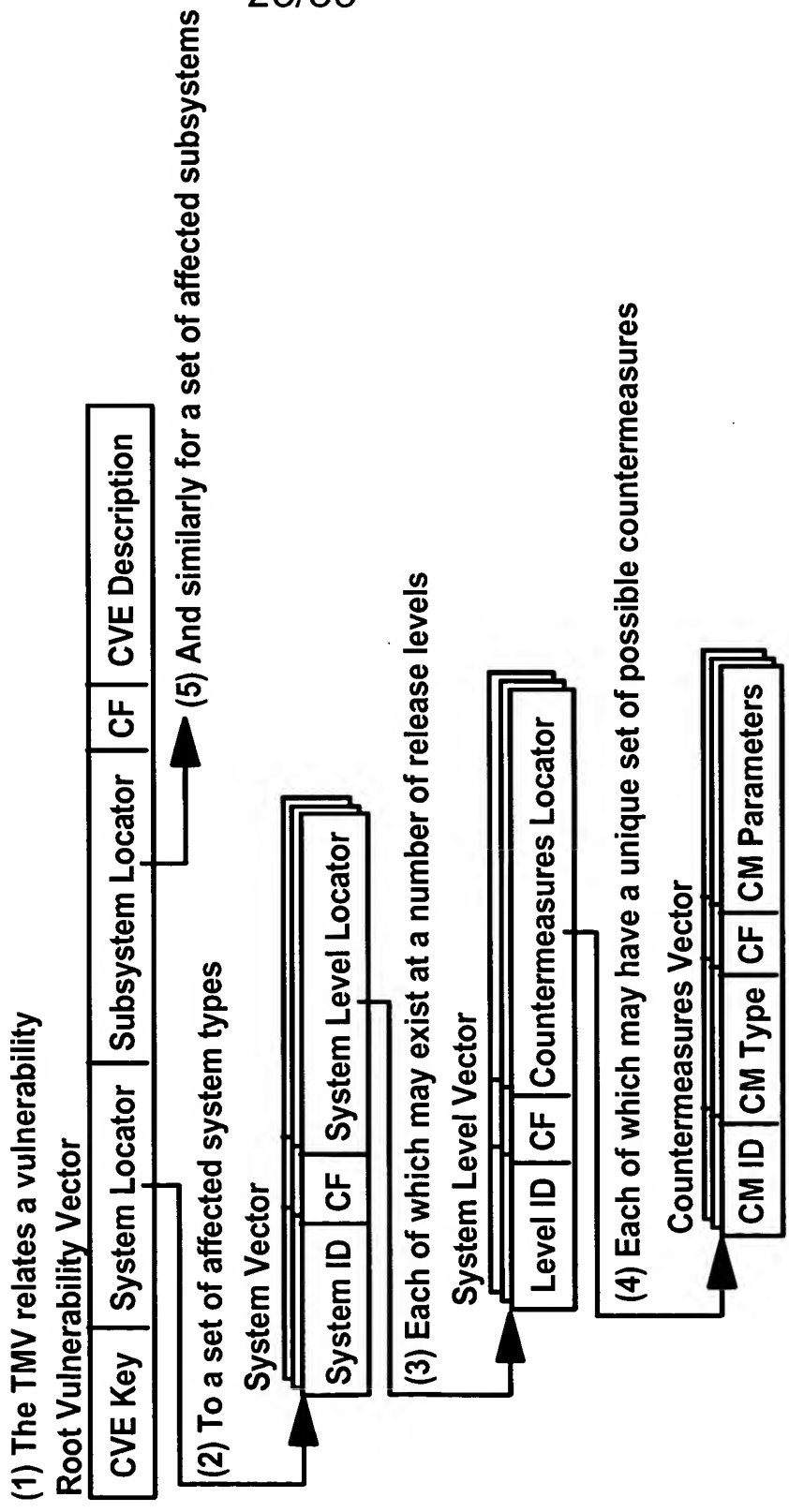

(1) The TMV relates a vulnerability
Root Vulnerability Vector
CVE Key
System Locator
Subsystem Locator
CF
CVE Description
(2) To a set of affected system types
System Vector
System ID
CF
System Level Locator
(3) Each of which may exist at a number of release levels
System Level Vector
Level ID
CF
Countermeasures Locator
(4) Each of which may have a unique set of possible countermeasures
Countermeasures Vector
CM ID
CM Type
CF
CM Parameters
(5) And similarly for a set of affected subsystems

FIG. 31

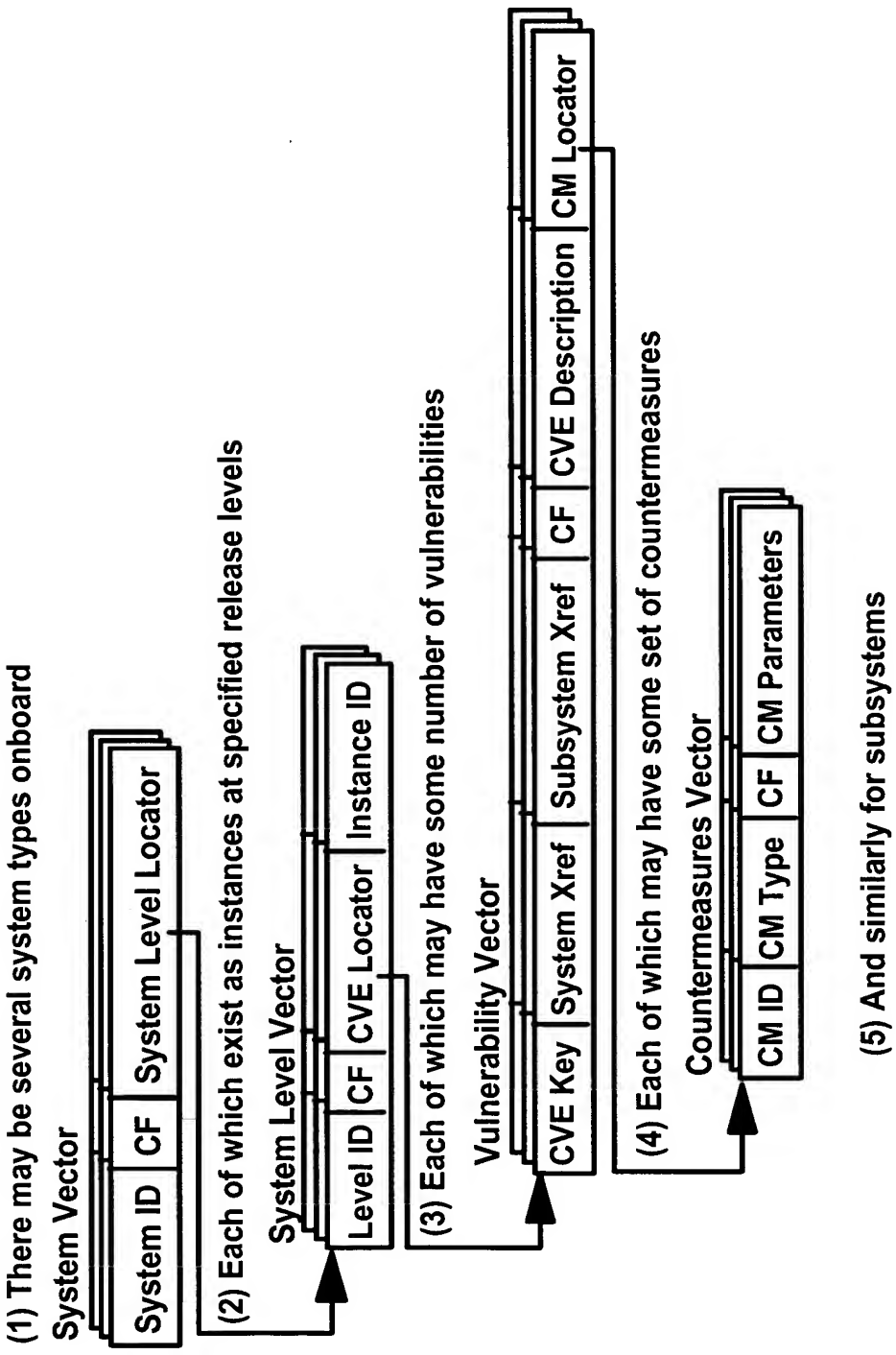

(1) There may be several system types onboard
System Vector
System ID
CF
System Level Locator
(2) Each of which exist as instances at specified release levels
System Level Vector
Level ID
CF
CVE Locator
Instance ID
(3) Each of which may have some number of vulnerabilities
Vulnerability Vector
CVE Key
System Xref
Subsystem Xref
CF
CVE Description
CM Locator
(4) Each of which may have some set of countermeasures
Countermeasures Vector
CM ID
CM Type
CF
CM Parameters
(5) And similarly for subsystems

FIG. 32

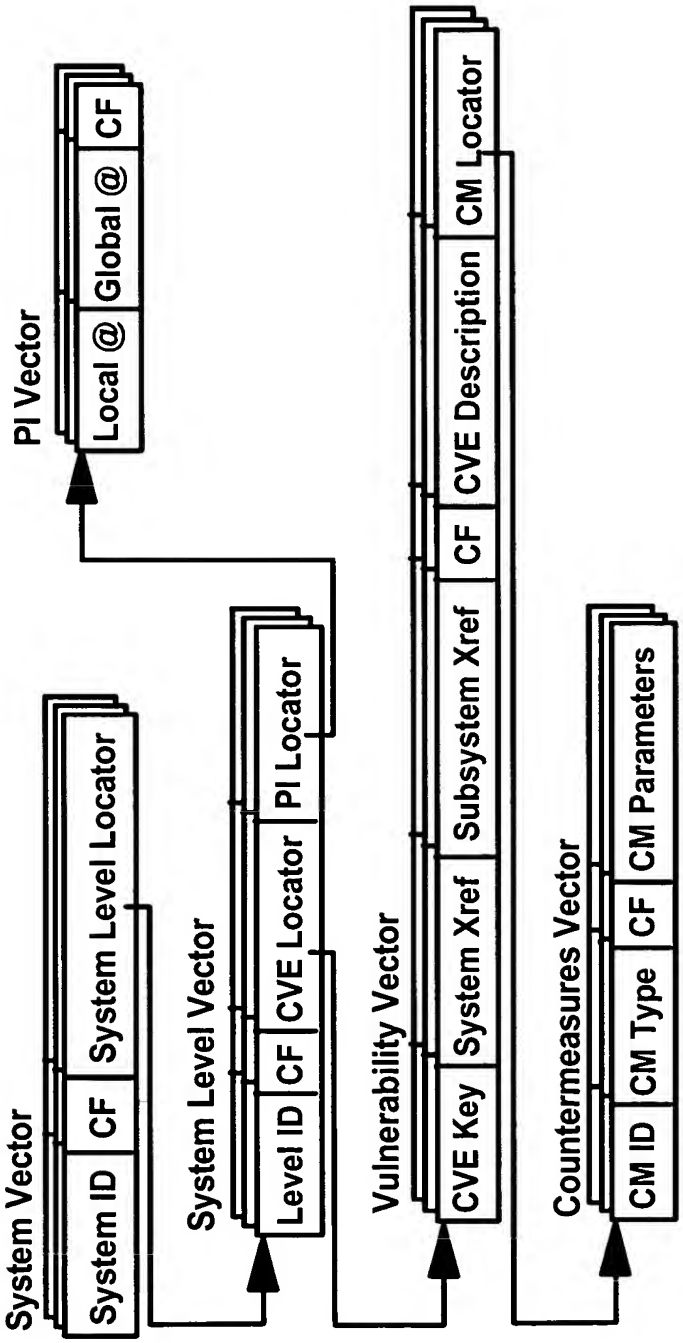

System Vector
System ID
CF
System Level Locator
System Level Vector
Level ID
CF
CVE Locator
PI Locator
PI Vector
Local @
Global @
CF
Vulnerability Vector
CVE Key
System Xref
Subsystem Xref
CF
CVE Description
CM Locator
Countermeasures Vector
CM ID
CM Type
CF
CM Parameters

FIG. 33A

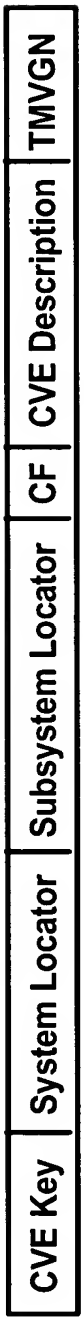


FIG. 33B

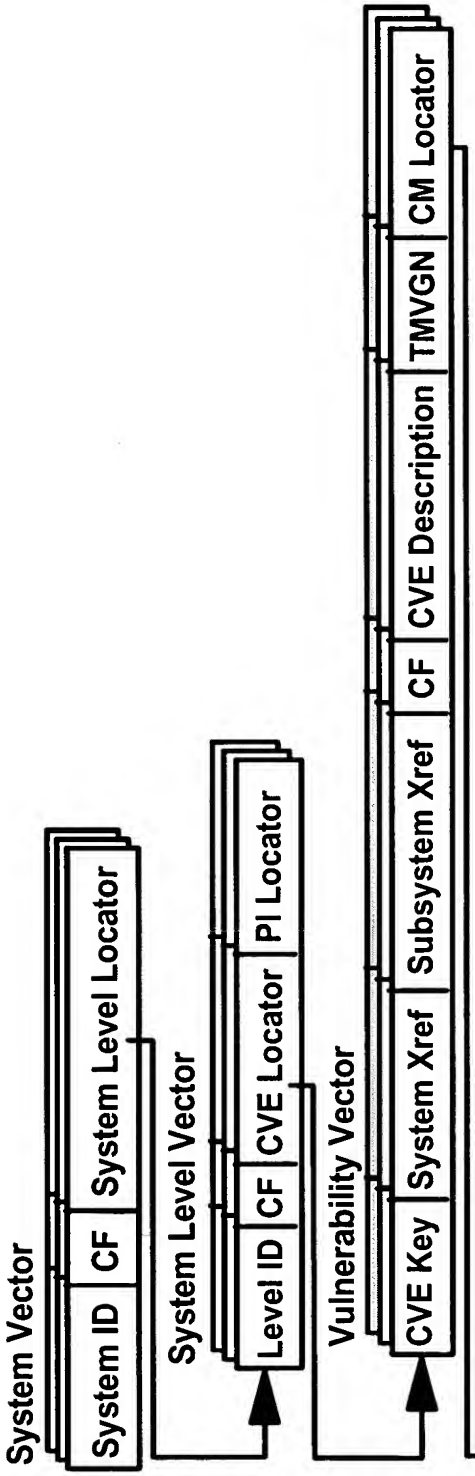


FIG. 33C

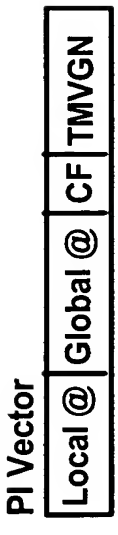


FIG. 34

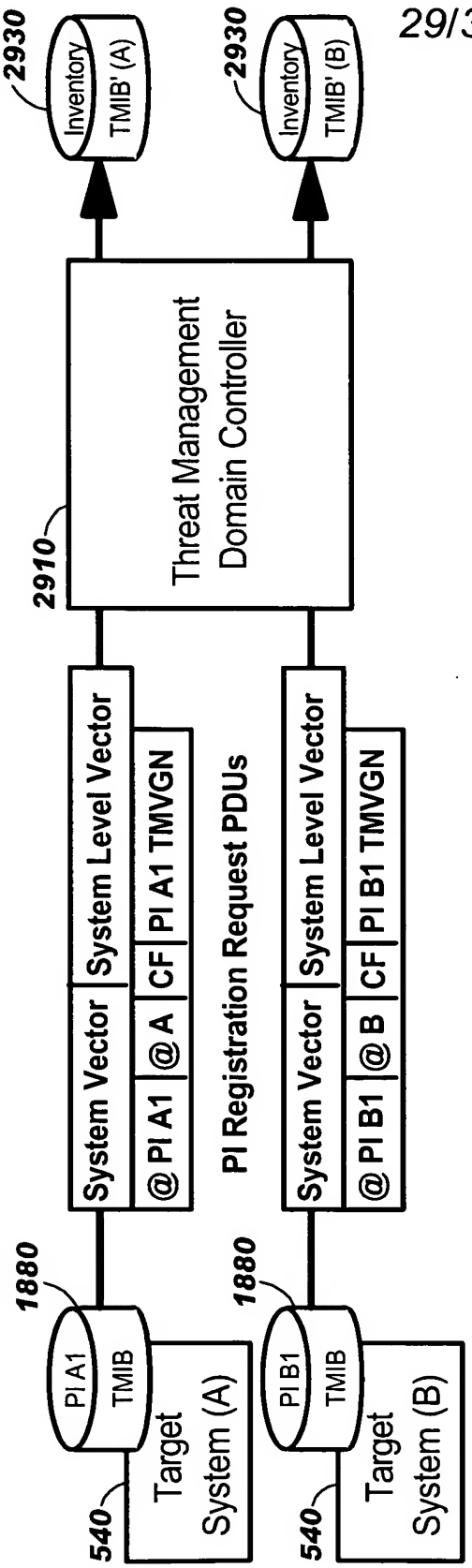

2930
Inventory
TMIB' (A)
2930
Inventory
TMIB' (B)
2910
Threat Management
Domain Controller
System Vector
@ PI A1
@A
CF
PI A1 TMVGN
System Level Vector
PI Registration Request PDUs
System Vector
@ PI B1
@B
CF
PI B1 TMVGN
System Level Vector
1880
PI A1
TMIB
1880
PI B1
TMIB
540
Target
System (A)
540
Target
System (B)

FIG. 35

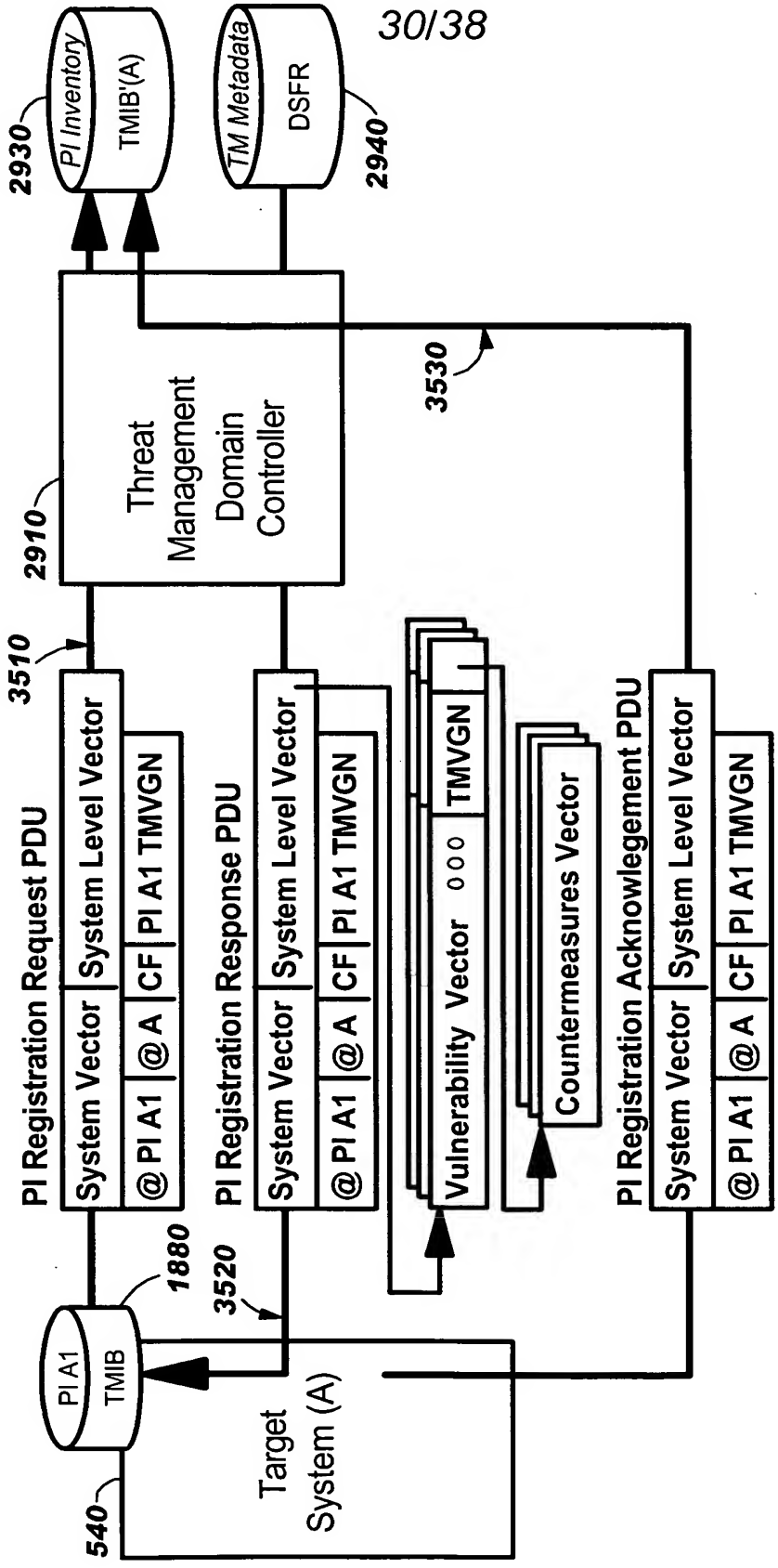
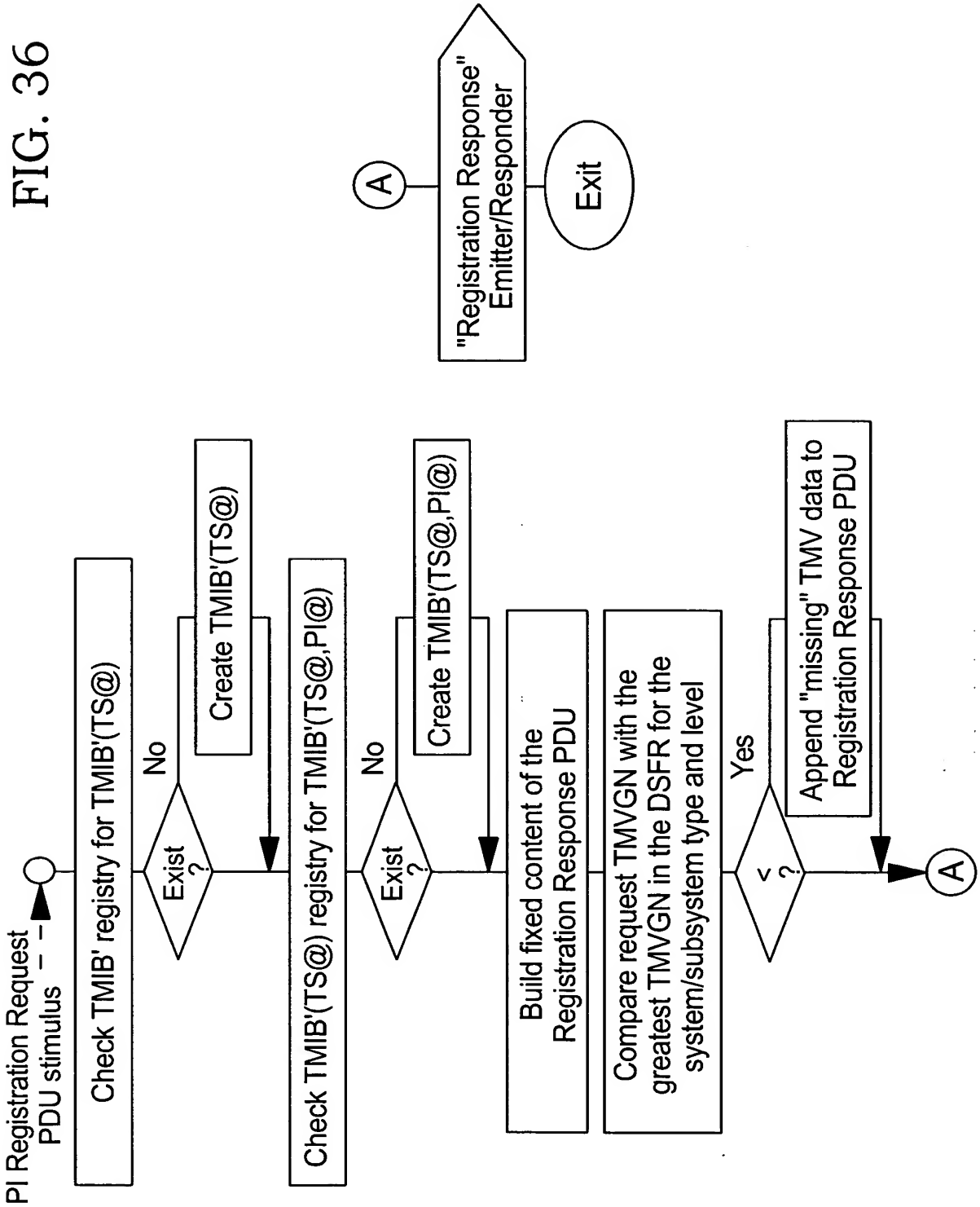

PI Inventory
TMIB'(A)
2930
TM Metadata
DSFR
2940
Threat Management Domain Controller
2910
3530
3510
PI Registration Request PDU
System Vector
System Level Vector
@ PI A1
@ A
CF
PI A1 TMVGN
PI Registration Response PDU
System Vector
System Level Vector
@ PI A1
@ A
CF
PI A1 TMVGN
Vulnerability Vector
TMVGN
Countermeasures Vector
PI Registration Acknowlegement PDU
System Vector
System Level Vector
@ PI A1
@ A
CF
PI A1 TMVGN
1880
3520
PI A1
TMIB
Target System (A)
540

FIG. 36


PI Registration Request PDU stimulus
Check TMIB' registry for TMIB'(TS@)
Exist ?
No
Create TMIB'(TS@)
Check TMIB'(TS@) registry for TMIB'(TS@,PI@)
Exist ?
No
Create TMIB'(TS@,PI@)
Build fixed content of the Registration Response PDU
Compare request TMVGN with the greatest TMVGN in the DSFR for the system/subsystem type and level
< ?
Yes
Append "missing" TMV data to Registration Response PDU
A
A
"Registration Response" Emitter/Responder
Exit

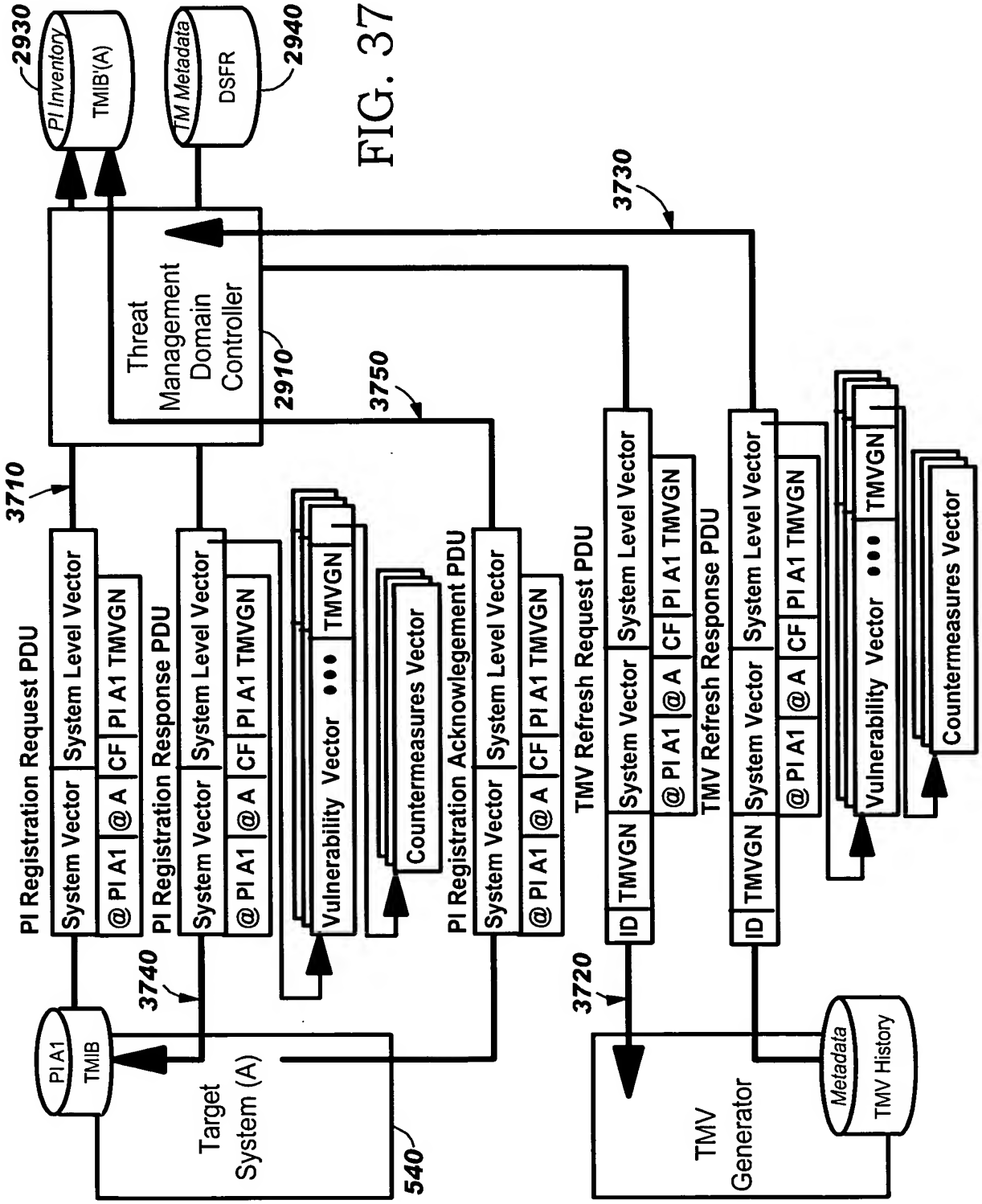

2930
PI Inventory
TMIB'(A)
2940
TM Metadata
DSFR
Threat Management Domain Controller
2910
3710
3730
3750
PI Registration Request PDU
System Vector
System Level Vector
@ PI A1
@ A
CF
PI A1 TMVGN
PI Registration Response PDU
Vulnerability Vector
TMVGN
Countermeasures Vector
PI Registration Acknowlegement PDU
TMV Refresh Request PDU
ID
TMV Refresh Response PDU
3740
3720
PI A1
TMIB
Target System (A)
540
TMV Generator
Metadata
TMV History

FIG. 37

FIG. 38

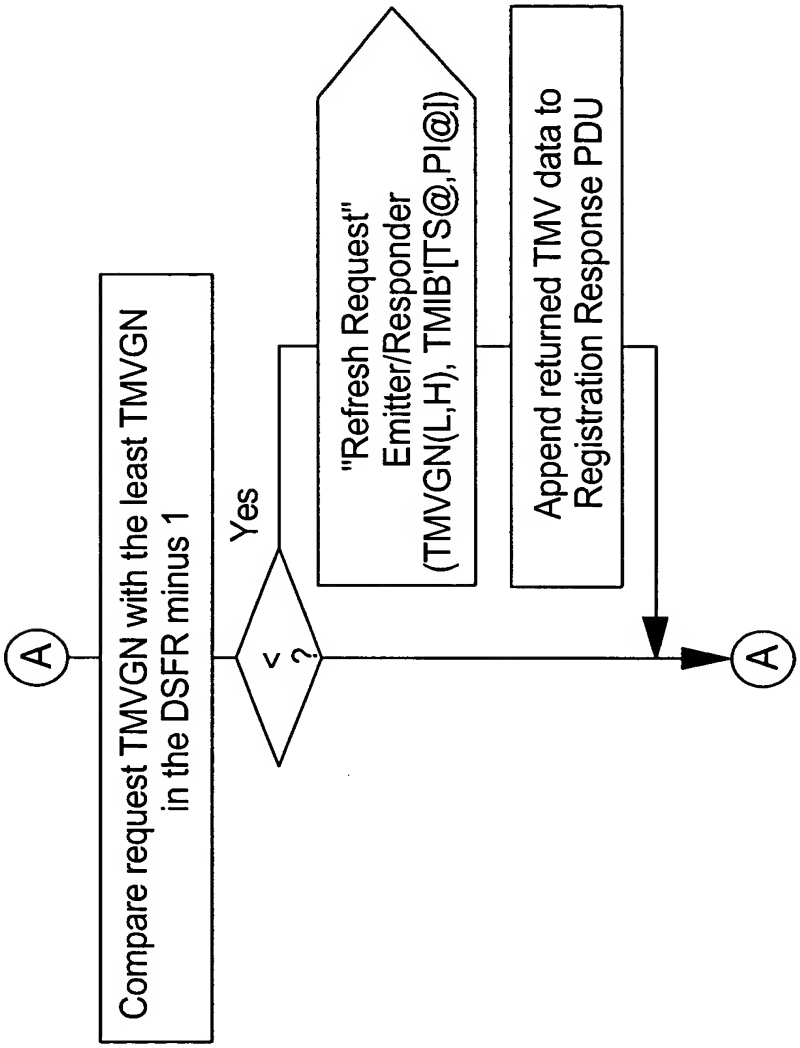

A
Compare request TMVGN with the least TMVGN in the DSFR minus 1
v ?
Yes
"Refresh Request" Emitter/Responder (TMVGN(L,H), TMIB'[TS@,PI@])
Append returned TMV data to Registration Response PDU
A

FIG. 39

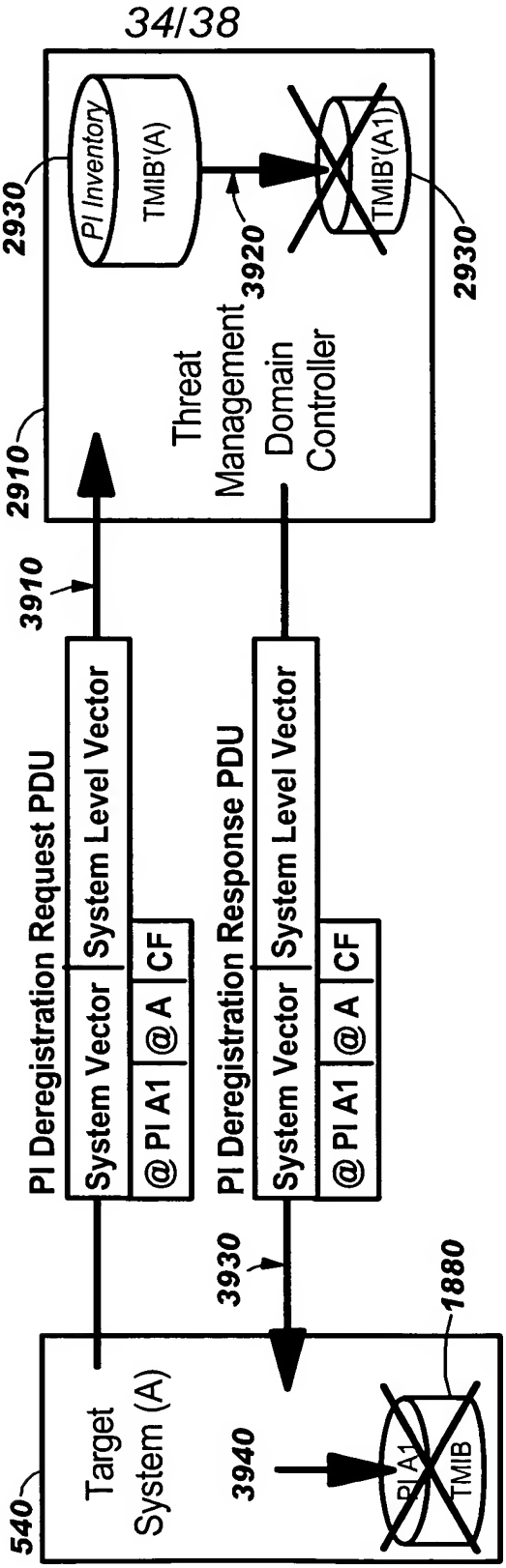

2930
PI Inventory
TMIB'(A)
TMIB'(A1)
2930
3920
Threat Management Domain Controller
2910
3910
PI Deregistration Request PDU
System Vector
System Level Vector
@ PI A1
@ A
CF
PI Deregistration Response PDU
System Vector
System Level Vector
@ PI A1
@ A
CF
3930
1880
Target System (A)
3940
PI A1
TMIB
540

FIG. 40

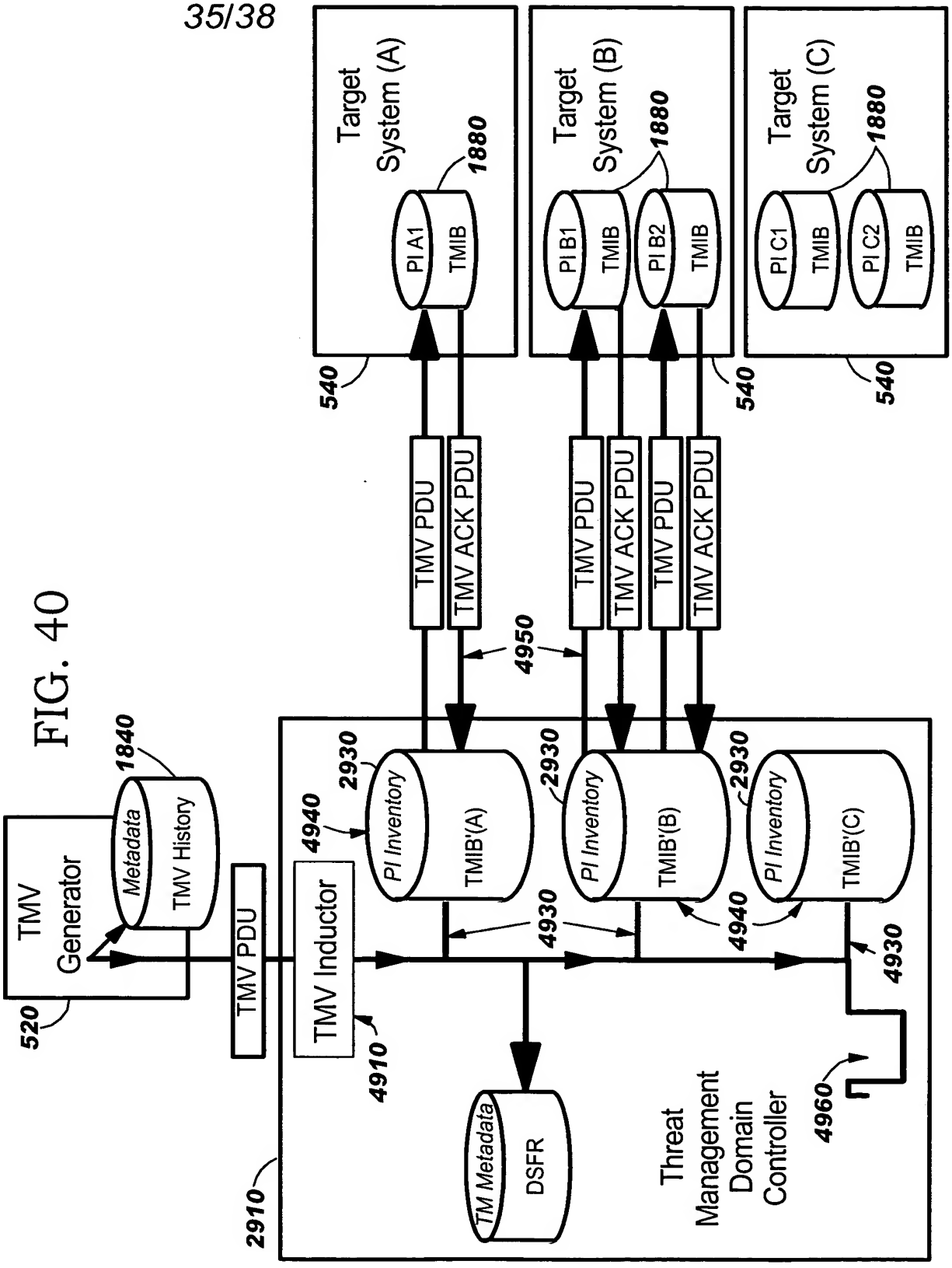

Target System (A)
Target System (B)
Target System (C)
1880
PI A1
TMIB
PI B1
PI B2
PI C1
PI C2
540
TMV PDU
TMV ACK PDU
4950
TMV Generator
Metadata
TMV History
1840
520
TMV PDU
TMV Inductor
4910
2930
4940
PI Inventory
TMIB'(A)
TMIB'(B)
TMIB'(C)
4930
TM Metadata
DSFR
Threat Management Domain Controller
2910
4960

FIG. 41

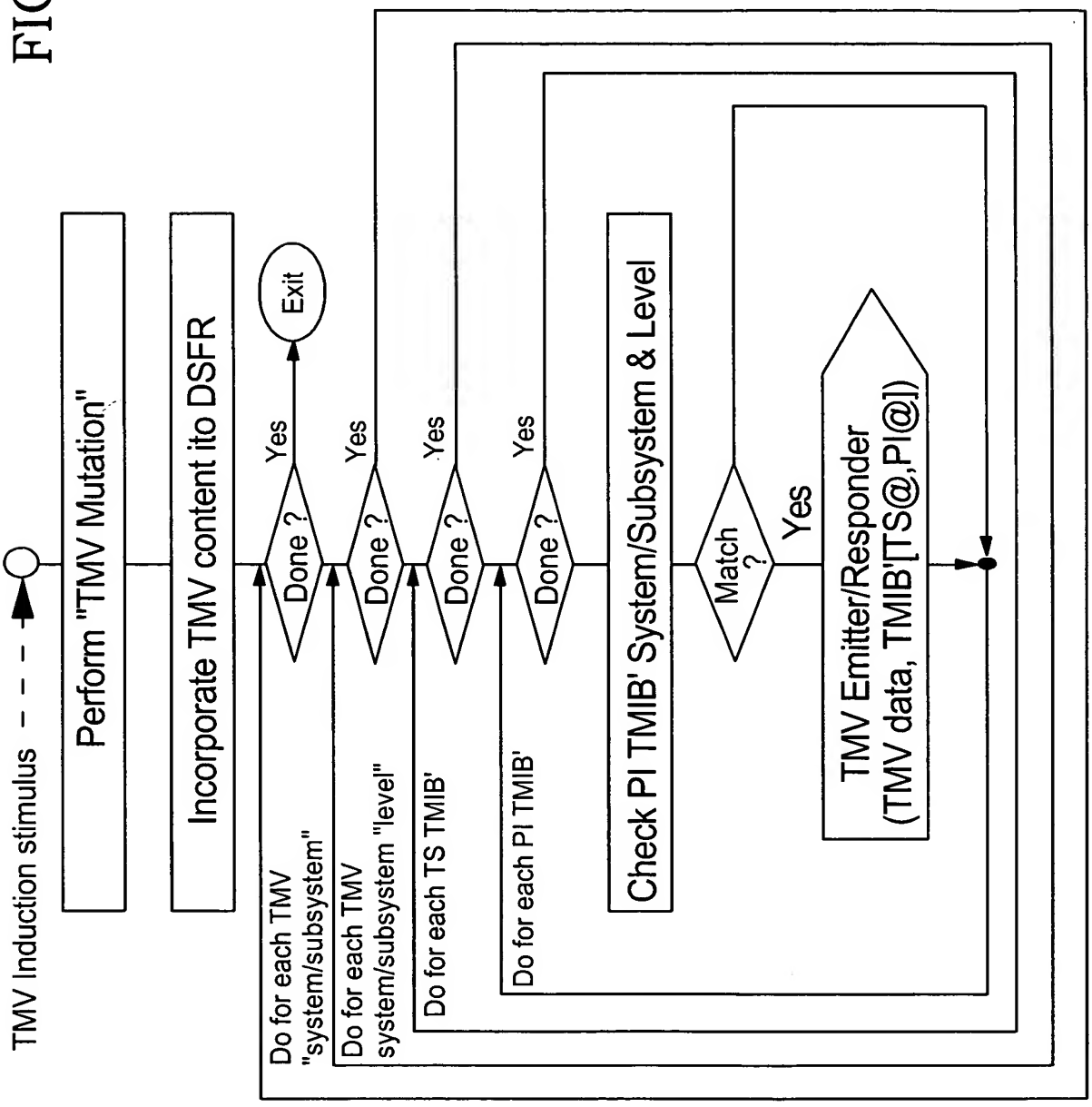

TMV Induction stimulus
Perform "TMV Mutation"
Incorporate TMV content ito DSFR
Do for each TMV "system/subsystem"
Done ?
Yes
Exit
Do for each TMV system/subsystem "level"
Done ?
Yes
Do for each TS TMIB'
Done ?
Yes
Do for each PI TMIB'
Done ?
Yes
Check PI TMIB' System/Subsystem & Level
Match ?
Yes
TMV Emitter/Responder (TMV data, TMIB'[TS@,PI@])

FIG. 42A

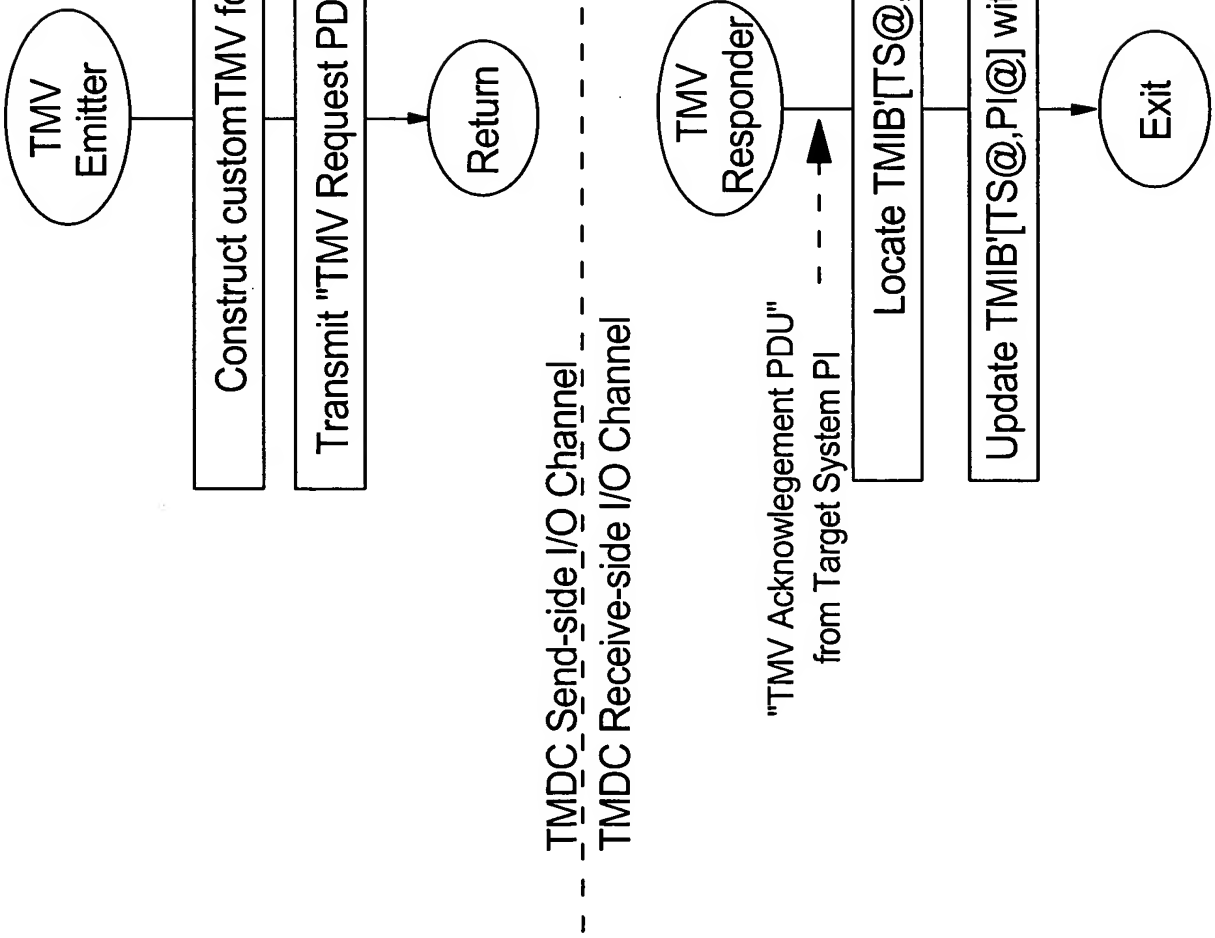
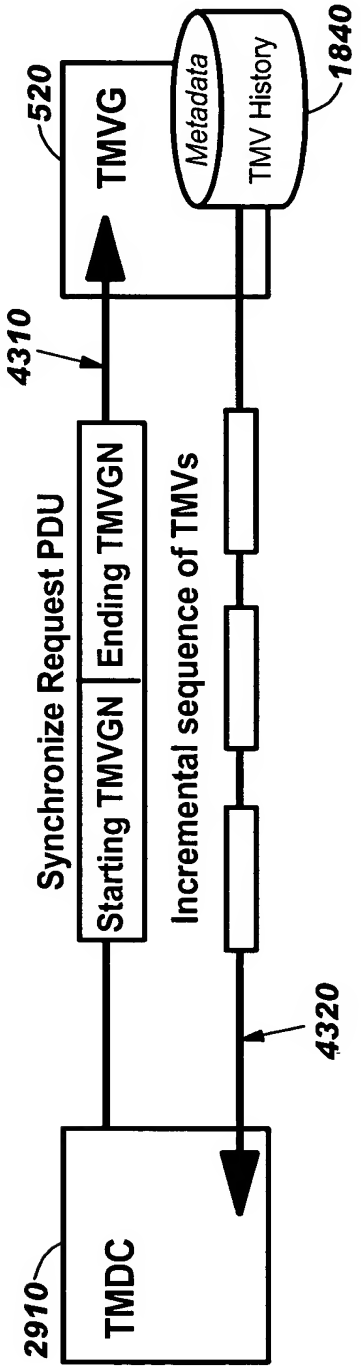


FIG. 42B

FIG. 43


520
TMVG
Metadata
TMV History
1840
4310
Synchronize Request PDU
Starting TMVGN
Ending TMVGN
Incremental sequence of TMVs
4320
2910
TMDC